INFORMATION SHARING ENVIRONMENT (ISE)

SUSPICIOUS ACTIVITY REPORTING (SAR) EVALUATION ENVIRONMENT (EE) SEGMENT ARCHITECTURE

Prepared by the
Program Manager, Information Sharing Environment

Version 1, December 2008

INFORMATION SHARING ENVIRONMENT (ISE)

SUSPICIOUS ACTIVITY REPORTING (SAR) EVALUATION ENVIRONMENT (EE) SEGMENT ARCHITECTURE

Prepared by the
Program Manager, Information Sharing Environment

Version 1
December 2008

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Overview

The Program Manager, Information Sharing Environment (PM-ISE) is sponsoring an Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Evaluation Environment (EE) in furtherance of nationwide sharing of Suspicious Activity Reports (SARs) determined to or deemed to have a potential terrorism nexus[1]. The ISE-SAR EE project extends current SAR activities in the ISE to support examination of a variety of operational ISE-SAR-related processes, such as law enforcement information gathering, processing, coordination, outreach/liaison, vetting and analysis, reporting, associated training, and facilitation. The ISE-SAR EE will also explore the benefits of training front line and supervisory law enforcement personnel regarding recognized behaviors and incidents associated with terrorism-related criminal activity. Finally, the project will focus on enhancing interconnectivity of systems to better enable sharing of ISE-SAR data.

Benefits from this ISE-SAR EE effort will include inputs for the development and publication of a guide or template for Federal, and State, local and tribal (SLT) entities to use in establishing policies, common business processes, architectures, and technical capabilities for gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity information. Results will also be used to provide updates to the *ISE-SAR Functional Standard*. Standardizing a SAR approach across the various levels of government will help meet the following objectives:

A. Develop and document standing and threat-based priority information needs that will, once combined with existing national and regional needs, fully inform the gathering of terrorism-related SARs for a State or local area. These priority information needs will be developed through a coordinated information sharing effort involving Federal, State and local authorities at both a national and SLT level;

B. Gather, document, process, vet, make available, share, and use terrorism-related SARs by individual local law enforcement entities with the Joint Terrorism Task Forces (JTTFs) and Fusion Centers in a manner that ensures the appropriate operational and analytical responses while protecting the information privacy and legal rights of Americans;

C. Federal field elements, regional and/or major urban area law enforcement entities post terrorism-related SARs in ISE Shared Spaces.

These objectives cover the life cycle of ISE-SAR activity and reflect the need for an evaluation environment to help develop and test various business processes and procedures; to help identify and address a range of policy issues; and to assess selected architectural and technical concepts supporting the business processes, procedures, and policies associated with a nationwide SAR capability.

[1] Throughout this *ISE-SAR EE Segment Architecture* document, where terrorism-related SARs are cited in the text, this implies that the SAR information is *determined to or deemed to have a potential terrorism nexus* through the processes outlined in the *ISE-SAR Functional Standard*.

Presented in this document is a logically arranged compilation of business and functional drivers for the ISE-SAR EE project. This information is based on current ISE-SAR EE documents, related ISE documentation, and general ISE concepts (reference Section 2.5 for applicable source and compliance documentation). This Segment Architecture document lays the foundation for building an executable operational information technology (IT) solution for the ISE-SAR EE that meets or exceeds mission performance goals. It achieves this by documenting those sets of business and information requirements, outcomes, and constraints that drive necessary decisions (both programmatic and solution) consistent with the business case for the ISE-SAR EE.

This Segment Architecture describes business and functional outcomes for the ISE-SAR EE delineated as either "Threshold" or "Objective." *Threshold* outcomes represent the *minimum* capability needed within the evaluation environment to support assessment and refinement of business processes, procedures, architectural elements, and policies for the ISE-SAR EE. *Objective* outcomes identify additional capabilities to those Threshold outcomes that are targets for achievement pending ISE-SAR EE resource (people, funding) and time availability. Objective outcomes also represent growth capabilities that are not required for the ISE-SAR EE but are deemed beneficial and desired if they can be incorporated within the existing ISE-SAR EE funding and schedule constraints. The *ISE-SAR EE Solution Architecture*, developed subsequent to and consistent with this Segment Architecture, will leverage existing capabilities when appropriate, and will document which business and functional capabilities will be Threshold or Objective for implementation, primarily based upon resource availability.

A similar construct exists for the business challenges being evaluated as part of the ISE-SAR EE. Threshold outcomes, as related to the SAR business process, represent the minimum level of performance that, if achieved, would support a conclusion that the business process, procedure, or policy position as it exists or has evolved is sufficiently defined and accepted to feed into a broader, longer term SAR Segment Architecture for the ISE. Failure to meet this level of performance could justify continuation of the ISE-SAR EE to further refine and evaluate the business processes, procedures, and policy positions. Appendix A provides a summary of both the identified Threshold and Objective outcome needs for the ISE-SAR EE identified throughout this document.

This Segment Architecture document is intended for senior leadership, program managers, Chief Architects, systems designers, network managers, and IT implementers associated with the ISE-SAR EE project. This document was developed through a collaborative, integrated project team consisting of SAR business subject matter experts, enterprise architects, and IT subject matter experts from Information Sharing Council[2] and State/local community representatives to include the ISE-SAR Steering Committee. Future versions of this document, if necessary, will be informed and updated by the ISE-SAR EE outcomes.

[2] The Information Sharing Council was established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection 1016(g) of the Intelligence Reform and Terrorism Prevention Act (IRTPA). [Extracted from IRTPA 1016(a)(1)] EO 13388, which superseded EO 13356, established the Information Sharing Council.

2 Introduction

The PM-ISE is sponsoring an ISE-SAR EE involving two projects: (1) a library (designated throughout this document as the "SAR Summary Reports Library") of free-text SAR summary reports (containing no personal information) from a variety of sources and (2) an evaluation using ISE Shared Spaces to store (or provide access to) and share SARs deemed to have a terrorism nexus.[3] For the purposes of this ISE-SAR EE, ISE Shared Spaces will support information sharing in the Controlled Unclassified Information (CUI) security domain. This project will test the assumptions of sharing SAR information following the *ISE-SAR Functional Standard* (ISE-FS-200)[4] across multiple communities: State and local law enforcement agencies, State and major urban area fusion centers,[5] and Federal law enforcement (U.S. Department of Justice [DoJ], the U.S. Department of Defense [DoD] Antiterrorism/Force Protection, Federal Bureau of Investigation [FBI], and the U.S. Department of Homeland Security [DHS]).

This ISE-SAR EE will also examine the usefulness of the ISE-SAR Criteria Guidance (Part B of the *ISE-SAR Functional Standard*) and the sharing of ISE-SAR information among major city and county law enforcement agencies, State and major urban area fusion centers, and Federal Government agencies. This ISE-SAR EE, following best programmatic and systems engineering practices, is being developed in a manner that provides a foundation to shape the longer-term information sharing capability for the ISE.

For this ISE-SAR EE, participants will assess the process of designating information as an ISE-SAR, the value of the ISE-SAR information (including the value of including personal information), the rules for providing access to the ISE-SAR information, and the utility of technical feedback mechanisms for the developer or the search tool. An evaluation report is planned for the project. The specific evaluation criteria and measurement techniques will be also described in a Performance Plan prior to operational use of the ISE-SAR EE capabilities.

[3] The *ISE Enterprise Architecture Framework, Version 2.0* describes "ISE Shared Spaces" as networked data and information repositories used to make standardized terrorism-related information, applications, and services accessible to all ISE participants (across the communities of law enforcement, homeland security, intelligence, defense, and foreign affairs) in each of the three ISE security domains—Controlled Unclassified Information (CUI), Secret, and Sensitive Compartmented Information (SCI). The *ISE EAF* introduced this concept of "ISE Shared Spaces" to help resolve the information processing and usage problems identified by the 9/11 Commission and the IRTPA. The ISE Shared Spaces concept defines the infrastructure layout to allow ISE participants operating on national security systems (NSS) to exchange information with participants on non-NSS networks, and defines the means for foreign partners to interface and share terrorism information with U.S. counterparts. For the purposes of this ISE-SAR EE, ISE Shared Spaces will support information sharing in the CUI security domain. Detailed implementation guidance on planning and implementing an ISE Shared Space is also provided in Appendix D. The *ISE EAF* may be accessible from www.ise.gov under the ISE Architecture Program section.

[4] The *ISE-SAR Functional Standard*, including cover document and technical artifacts, may be accessible from www.ise.gov under the Common Terrorism Information Sharing Standards (CTISS) Program section.

[5] The *National Strategy for Information Sharing* defines a major urban area fusion center as a regional fusion center established by localities participating in an urban area security initiative (UASI).

The development of a nationwide SAR process is called for in the *National Strategy for Information Sharing (NSIS)*,[6] and with specific responsibilities for Federal and SLT officials laid out in the NSIS Appendix. This ISE-SAR EE will be used to help develop and assess the integrated Federal, and SLT process components comprising a nationwide SAR capability as documented in the *Nationwide Suspicious Activity Reporting Initiative* (*NSI): CONOPS*. The importance of this effort, as well as the nature of the topic, is of interest to the public. Therefore, keeping the public informed is an important part of the SAR process and is so stated in the *Findings and Recommendations of the SAR Support and Implementation Project*.

To ensure information is communicated consistently and accurately, the PM-ISE Outreach and Communications team will routinely post information about the ISE-SAR EE on the public ISE website (www.ise.gov). Currently the PM-ISE coordinates with the ISE-SAR EE partners to address public affairs related to the ISE-SAR EE, including talking points, fact sheets, and other documents intended to be made public. It is requested that media and press inquiries be directed to or coordinated with the Office of the PM-ISE.

2.1 Scope of the ISE-SAR EE Project

The specific scope of the ISE-SAR EE and of this Segment Architecture is the continuation and expansion of ongoing Nationwide Suspicious Activity Reporting evaluation and refinement activities identified in the *National Strategy for Information Sharing (NSIS)*.[7] The initial phase of the initiative involved the development of the SAR Summary Reports Library and the SAR supporting "ISE Shared Spaces" concept in Florida, Virginia, and New York. As Figure 2-1 depicts, this initial phase was intended to develop and field, regionally, SAR nodes for structured SAR information using Web access and repositories (defined as SAR supporting "ISE Shared Spaces") at three State or major urban area fusion centers (indicated in blue), two of which are located near and working collaboratively with U.S. military installations working joint force protection.

[6] The *National Strategy for Information Sharing*, (Washington: White House, October 2007) may be accessible at www.whitehouse.gov/infocus/nationalstrategy and at www.ise.gov.

[7] White House, *National Strategy for Information Sharing*, Ibid., Appendix.

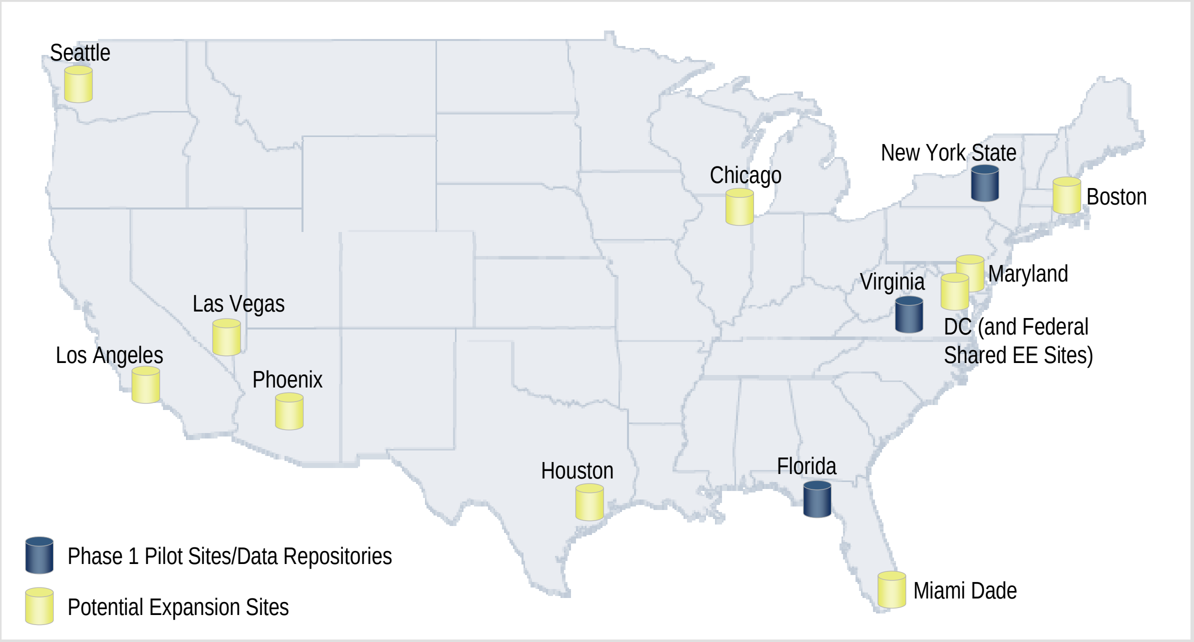


Figure 2-1. ISE-SAR EE Current and Potential Sites

The current, broader phase of the project will continue the evaluation and refinement process and expands connectivity to include up to a maximum of 10 additional sites (indicated in yellow in Figure 2-1) which will utilize a consistent approach to law enforcement information gathering, outreach/liaison, vetting, reporting, associated training, and facilitation. SAR information made available to authorized ISE-SAR EE participants will be provided by local or tribal law enforcement, State agencies, or field elements of Federal agencies and tracked within systems built and maintained by Federal and SLT authorities. The initiative requires adoption of a process for determining the kinds of behavior and incidents associated with terrorism-related criminal activity implementing common solutions at each implementation site, and determining the need for potential enhancements of supported technology to enable sharing of SAR data.

The ISE-SAR EE explores various challenges associated with implementation of a nationwide SAR capability. Existing systems provide much of the baseline for the project, but the environment additionally leverages the “ISE Shared Spaces” and ISE Core Services architectural concepts identified within the *ISE Enterprise Architecture Framework (EAF)* including a federated search capability. The new capabilities provided for in the ISE-SAR EE are bounded by business processes on both the supplier and user side of the SAR life cycle. On the supplier side, the boundary is represented by the upload of data from ISE-SAR EE participant holdings to an ISE Shared Space. On the user side, the boundary is represented by the ability to access an ISE Shared Space search capability, issue a federated query across ISE Shared Spaces, and receive results in response to that query. External to these boundaries, the primary focus is on business processes, procedures, and policies[8]. These include but are not limited to

[8] See Section 4 for the detailed description of the SAR process.

A. SLT threat/risk assessment and integration of the identified SLT information needs with Federal information needs to produce a consolidated set of national priority information needs;

B. Issuance of criteria for recognizing potential terrorism-related activity, to be utilized across all levels of government;

C. Information gathering and reporting from Federal field units and SLTs to JTTFs and Fusion Centers; and

D. Allocation of responsibilities for national-level, regional, and jurisdictional analysis of ISE-SAR information.

Protection of privacy and civil liberties is a major consideration for this ISE-SAR EE and, as such, warrants special attention. Additional information on privacy and civil liberties protections is located in Section 5.1 of this document.

2.2 ISE-SAR EE Participating Organizations and Proposed EE Sites

The ISE-SAR EE is sponsored and funded by the PM-ISE who is responsible for overall direction and oversight. The Department of Justice's Bureau of Justice Assistance (DoJ/BJA) provides planning, project management, and implementation services. The Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD HD&ASA) participates in support of the DoD force protection mission. DHS fusion center representatives will support ISE-SAR activities at participating sites. In addition, at least one DHS component organization will implement an ISE Shared Space that will be accessible by other ISE-SAR EE participants. The FBI will participate in the ISE-SAR EE primarily through its JTTFs, some of which are collocated with fusion centers. In addition to these Federal organizations, the Criminal Intelligence Coordinating Council (CICC), the International Association of Chiefs of Police (IACP), the Major City Chiefs' Association (MCCA), and the Major County Sheriffs' Association (MCSA) will provide a consolidated State and local perspective.

The following States and cities are being considered as proposed ISE-SAR EE sites. The venues listed are being considered because of a number of factors, including involvement in the MCCA SAR Support and Implementation Project (which developed several recommendations regarding implementation of the SAR process), level of technology, maturity of the Fusion Centers, and existing data efforts in the area of SARs. This list does not preclude the consideration of other States or cities as possible ISE-SAR EE participants.

- Boston (UASI)
- Houston (UASI)
- Las Vegas (UASI)
- Chicago/Illinois (UASI/State)
- Los Angeles/JRIC (UASI/State)
- Miami-Dade (UASI)
- Phoenix/Arizona (UASI/State)
- Seattle/Washington (UASI/State)

- Washington, DC (UASI) and Federal Shared EE Sites
- Maryland (State)
- Florida
- New York State
- Virginia

2.3 Definitions: Segment and Solution Architectures

A major challenge with identifying, implementing, and operating IT systems to support ISE mission processes, such as SAR, involves standardizing and rationalizing all the inherent differences and distinct separation of information resources[9] across the Federal Government and with SLT organizations where appropriate. Achieving business-led standardization and architectural integration is absolutely essential for establishing an ISE-SAR EE-wide, federated capability for efficiently, effectively, and reliably sharing ISE-SAR information. This document constitutes one of two documents being created by the ISE-SAR EE integrated project team.

Segment Architectures are logically arranged documents that lay the foundation for building executable operational solutions (or systems) that meet or exceed mission performance goals for a particular line of business and are derived from a concept of operations. Segment Architectures achieve this by documenting the set of business and information requirements, outcomes, and constraints. This *ISE-SAR EE Segment Architecture* document is scoped to one particular line of business—terrorism-related suspicious activity reporting. It documents the business outcomes and will drive necessary decisions (both programmatic and solution) consistent with the logical business case for the ISE-SAR EE.

Solution Architectures are structured, technical documents, *derived from Segment Architectures*, that are scoped to describe the particular functions or processes that will be implemented (in this case the SAR services and operations capabilities), identify methods for achieving operational outcomes, and define specific IT assets, applications, and components for procurement and implementation. Solution Architectures do not specifically identify vendors or specific vendor items as these are generally identified in subsequent specification documents and/or procurement orders. As part of this ISE-SAR EE, partnering ISE-SAR EE organizations will follow guidance from both this Segment Architecture and the corresponding *ISE-SAR EE Solution Architecture* to define ISE-SAR EE project development, implementation, and operations activities.

2.4 ISE Core Service Processes and the ISE-SAR EE

Service-based architectural concepts are the basis for IT planning in the ISE, and as such the ISE-SAR EE will be established following service-based concepts derived from the *ISE EAF*. For the purposes of this ISE-SAR EE, the main ISE Core Services from the *ISE EAF* to be implemented and demonstrated include

[9] 44 U.S.C. 3502(6) defines information resources as "information and related resources, such as personnel, equipment, funds, and information technology."

- *Discovery*: allows an ISE-SAR EE user to search for and locate existing services and data sources that can be accessed across the ISE-SAR EE following the services concept and implementation model of the ISE Portal;[10]
- *Security*: provides mechanisms to the users of the ISE-SAR EE by supporting authentication, authorization, and access control processes;
- *Mediation*: helps bridge disparate information exchanges and systems between data producers and consumers in the ISE-SAR EE to include data transformation and adaptation;
- *Enterprise Service Management*: provides continuous processes of managing, measuring, reporting, and improving the Quality of Service (QoS) of ISE-SAR EE systems and applications;
- *Storage*: includes data source integration and enterprise content delivery networking; and
- *Collaboration*: enables communication and file-sharing among ISE-SAR EE users and may aid users to discover other users based on availability, knowledge, and skills.

The ISE Portal services concept from the *ISE EAF*, logically instantiated and conceptually demonstrated by the interfaces established through the ISE-SAR EE, describes the primary delivery mechanism for portal-type services in the ISE Core. In some cases, the ISE Portal concept is simply a user interface to underlying ISE Core Services. The ISE Portal services concept, as instantiated in the ISE-SAR EE, is implemented using commercial portal technology and provides ISE-SAR EE users access to common functionality such as user interface, portal management, publish/subscribe, and user assistance. Throughout the following sections, ISE Core and ISE Portal services are cited along with the descriptions, outcomes, affected processes, and constraints for focused, enabling service areas of the *ISE-SAR EE Segment Architecture*.

2.5 Applicable Source and Compliance Documentation

The following documents provide much of the basis and compliance requirements for the ISE-SAR EE:

- Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect Americans, (White House; October 2005)
- Findings and Recommendations of the Suspicious Activity Report (SAR): Support and Implementation Project, (Major City Chiefs Association [MCCA], GLOBAL, DOJ, DHS; June 2008) {Final Draft}
- Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines, (GLOBAL; September 2008)
- Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, (Global Justice Information Sharing Initiative [GLOBAL], DHS, DOJ); August 2006)
- Guidance Regarding the Use of Race in Law Enforcement Agencies, (DOJ, 2003)
- Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives, (GLOBAL) {Draft}

[10] Reference Chapter 6 of the *ISE EAF, Version 2.0* for more details on the ISE Portal concept.

- ISE Enterprise Architecture Framework (EAF), Version 2.0, (Office of the PM-ISE; September 2008)
- ISE-FS-200: ISE Functional Standard Suspicious Activity Reporting, Version 1.0, (Office of the PM-ISE; January 2008)
- *ISE Implementation Plan*, (Office of the PM-ISE; November 2006)
- *ISE Privacy Guidelines*, (Office of the PM-ISE; December 4, 2006)
- ISE Profile and Architecture Implementation Strategy (PAIS), Version 1.0, (Office of the PM-ISE; May 2008)
- ISE-SAR EE Implementation Guide (DOJ/BJA, 2008) {Draft}
- ISE-SAR Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis, (Office of the PM-ISE; September 2008)
- Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information (CUI), (White House; May 9, 2008)
- Memorandum of Understanding (MOU) between DOJ/BJA and PM-ISE, (July 2008)
- National Strategy for Information Sharing, (White House; October 2007)
- Nationwide Suspicious Activity Reporting Initiative: Concepts of Operations, Version 1.0, (Office of the PM-ISE; December 2008)
- Privacy and Civil Liberties Implementation Guide for the ISE, Version 1.0, (Office of the PM-ISE; September 2007)
- Protecting Civil Rights: A Leadership Guide for State, Local, and Tribal Law Enforcement, (International Association of Chiefs of Police; 2006)
- The National Criminal Intelligence Sharing Plan, (GLOBAL, DOJ/BJA); June 2005
- SAR: Proposal for Continuation and Expansion of National SAR Implementation and Regional SAR Analytical Collaboration Capabilities, (DOJ/Bureau of Justice Assistance (BJA); May 2008)

This page intentionally blank.

3 ISE-SAR EE Business Outcomes/Performance Goals

The following are the desired business outcomes for the ISE-SAR EE:

- Demonstration of the impact of a standardized, integrated approach to sharing terrorism-related suspicious activity;
- Assessment of the adequacy of the ISE-SAR process and its associated systems for achieving a nationwide SAR capability across all levels of government;
- Validation/refinement of the ISE-SAR process described in the *ISE-SAR Functional Standard*, including the information flow and criteria guidance; and
- Identification of processes to be validated; identification of processes to be developed; development and test of processes (to include process inputs, actions, products).

In order to assess performance against these outcomes, the ISE-SAR EE project team will use the following performance measures. These measures will therefore also allow the PM-ISE to gauge progress toward achieving this vision within the bounds of the environment.[11]

- General Progress:
    1. Number of participant locations that have established a formal process for gathering, documenting, processing, analyzing, and sharing terrorism-related SARs.
    2. Number of participant locations that have put in place a process for making terrorism-related SARs available to State and/or major urban area fusion centers and local JTTFs.
    3. Number of participant locations with privacy and civil liberties policies in place that meet or exceed the ISE Privacy Guidelines.
    4. Number of participant locations that have incorporated audits as part of their SAR process.
    5. Percentage of all sub-processes, constituting the steps of the Nationwide SAR process, that have been developed, validated, and tested.
    6. Number of full or part-time privacy officers added at supporting sites, as appropriate.
- Input:
    1. Number of State and/or major urban area fusion centers or other agencies submitting documents to the SAR Summary Reports Library.
    2. Number of State and/or major urban area fusion centers or other agencies that post terrorism-related SARs to an ISE Shared Space in a manner consistent with the *ISE-SAR Functional Standard.*

[11] At the direction of the National Security Council (NSC), the National Counterterrorism Center (NCTC) Directorate of Strategic Operational Planning (DSOP) has undertaken a critical analysis of the SAR process that will inform out-year budgeting across all Federal agencies. As part of this analysis, the NCTC proposed the following end state for the national SAR process: "By 2014, every Federal, State, local, tribal, and law enforcement entity operating domestically will participate in a standardized integrated approach to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity."

3. Number of Federal agencies that post terrorism-related SARs to an ISE Shared Space in a manner consistent with the *ISE-SAR Functional Standard*.

- Throughput:

1. Number of queries conducted both on the SAR Summary Reports Library and an ISE Shared Space.

- Outputs:

1. Number of products produced by the U.S. Government, intended to inform the SAR process, made available to State and/or major urban area fusion centers.
2. Number of State and/or major urban area fusion centers that establish a process for developing geographic risk assessments.
3. Number of geographic risk assessments completed or updated in the calendar year by State and/or major urban area fusion centers.
4. Number of State and/or major urban area fusion centers that have developed Priority Information Needs (PINs) as part of their geographic risk assessments.
5. Number of local personnel trained to recognize behaviors and indicators of terrorist activity (by job function).
6. Number of analytical products generated as a result of pattern and trend analysis of terrorism-related SARs.

- Outcomes:

1. Number of new individuals or groups identified as involved in terrorism-related crimes, including material support to terrorists, as a result of terrorism-related SARs.
2. Number of terrorist groups dismantled or disrupted as a result of terrorism-related SARs.
3. Number of investigations initiated as a result of terrorism-related SARs.
4. Number of investigations initiated as a result of terrorism-related SARs that result in arrests, convictions, or other law enforcement actions.
5. Number of enhancements to preparedness planning as a result of ISE-SAR-related threat analysis.
6. Number of enhancements to critical infrastructure protection as a result of ISE-SAR-related threat analysis.
7. Number of referrals to JTTF; number of investigative cases opened as result of the referral.

Using these measures, the ISE-SAR EE project team will determine whether the stated business outcomes have been achieved.

4 SAR Process

4.1 Nationwide SAR Process

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations* and shown in Figure 4-1, the nationwide SAR process involves a total of 12 discrete steps that are grouped under five general activity phases (planning, gathering and processing, analysis and production, dissemination, and reevaluation). It is important to note that this nationwide process identifies additional activities (which include training, information requirements determination, and risk assessments) that feed into the ISE-SAR process but are not specifically documented and modeled in other ISE-SAR documentation such as the *ISE-SAR Functional Standard*[12]. Consequently, the numbers indicated in Figure 4-1 only correlate to those nine-steps of the detailed information flow for nationwide SAR information sharing documented in version 1.0 of the *ISE-SAR Functional Standard.*

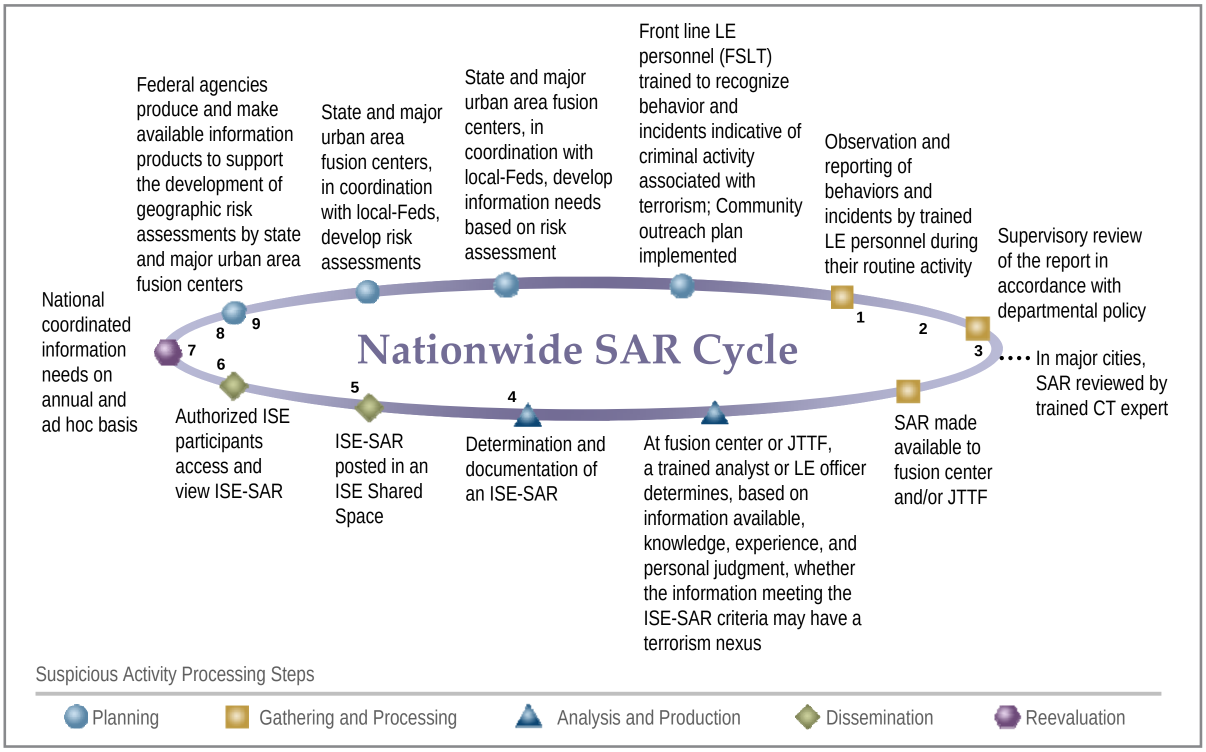

Nationwide SAR Cycle
Federal agencies produce and make available information products to support the development of geographic risk assessments by state and major urban area fusion centers
State and major urban area fusion centers, in coordination with local-Feds, develop risk assessments
State and major urban area fusion centers, in coordination with local-Feds, develop information needs based on risk assessment
Front line LE personnel (FSLT) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism; Community outreach plan implemented
Observation and reporting of behaviors and incidents by trained LE personnel during their routine activity
Supervisory review of the report in accordance with departmental policy
In major cities, SAR reviewed by trained CT expert
National coordinated information needs on annual and ad hoc basis
Authorized ISE participants access and view ISE-SAR
ISE-SAR posted in an ISE Shared Space
Determination and documentation of an ISE-SAR
At fusion center or JTTF, a trained analyst or LE officer determines, based on information available, knowledge, experience, and personal judgment, whether the information meeting the ISE-SAR criteria may have a terrorism nexus
SAR made available to fusion center and/or JTTF
1
2
3
4
5
6
7
8
9
Suspicious Activity Processing Steps
Planning
Gathering and Processing
Analysis and Production
Dissemination
Reevaluation

Figure 4-1. Overview of Nationwide SAR Process

[12] Detailed description of this 12-step Nationwide SAR process can be found in the *National Suspicious Activity Reporting Initiative: Concept of Operations*.

4.2 ISE-SAR Top-Level Business Process

A portion of the overall nationwide SAR process, the top-level ISE-SAR business process, focuses on the compilation, processing, and sharing of SAR information as shown in Figure 4-2; this business process is also described in detail in Section II of the *ISE-SAR Functional Standard*.[13] The ISE-SAR Top-level Business Process encompasses five standardized business process activities—Information Acquisition, Organizational Processing, Integration/ Consolidation, Data Retrieval/Distribution, and Feedback—each of which is discussed in detail throughout the following sections. The standardized business process description in the *ISE-SAR Functional Standard* was intentionally broad to include and accommodate all five ISE communities—intelligence, foreign affairs, homeland security, law enforcement, and defense. This section provides additional focused business outcomes and architectural details specific to the ISE-SAR EE in combating terrorism.[14]

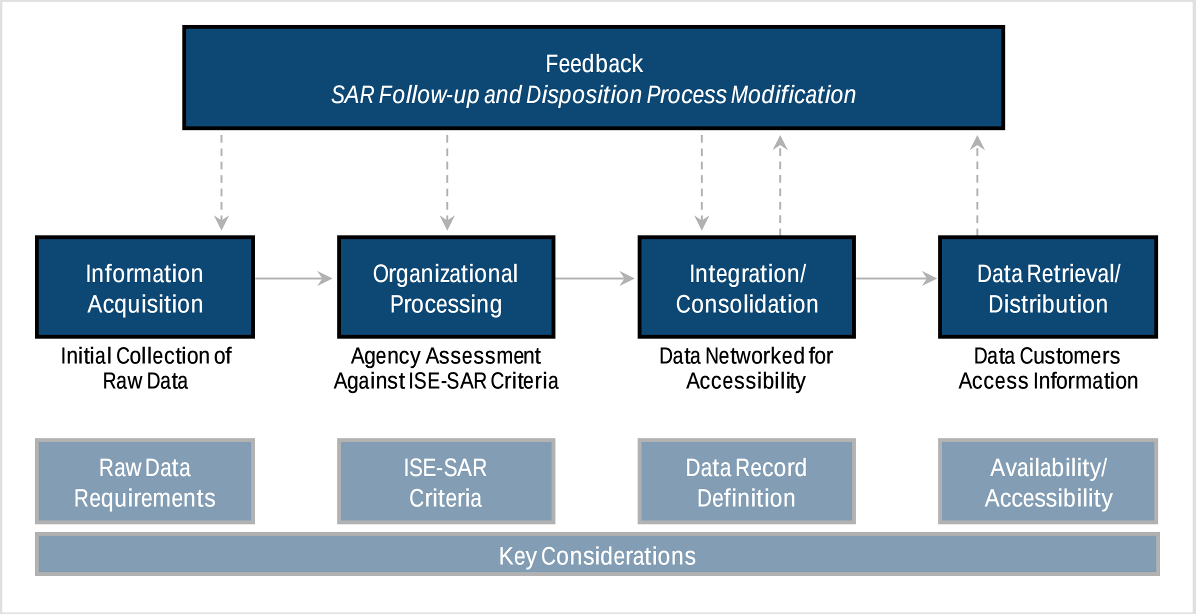

Feedback
SAR Follow-up and Disposition Process Modification
Information Acquisition
Initial Collection of Raw Data
Organizational Processing
Agency Assessment Against ISE-SAR Criteria
Integration/ Consolidation
Data Networked for Accessibility
Data Retrieval/ Distribution
Data Customers Access Information
Raw Data Requirements
ISE-SAR Criteria
Data Record Definition
Availability/ Accessibility
Key Considerations

Figure 4-2. ISE-SAR Top-level Business Process

From the *ISE-SAR Functional Standard*, suspicious activity reporting documents the observation of behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism-related crime. Such activities could include, but are not limited to, surveillance, photography of facilities and critical infrastructure, site breach or physical intrusion, cyber attacks, boats anchored in atypical locations, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemicals/agents or toxic materials, or other unusual behavior or sector-specific incidents. After one or more analytic reviews to verify and/or validate the information, those SARs that are determined to have a potential nexus to terrorism are designated as ISE-SARs

[13] *ISE-FS-200: ISE Functional Standard Suspicious Activity Reporting, Version 1.0* (Office of the PM-ISE; January 2008), 7-9.

[14] Although many of the organizations participating in the ISE-SAR EE use SARs to support an "all crimes" mission, the focus of this effort is on those SARs that have a potential nexus to terrorism.

and are processed, stored, shared, and used by ISE-SAR EE participants carrying out counterterrorism-related law enforcement missions.

In its most general usage, the term "suspicious activity report" does not refer to a particular form or type of document. Rather it describes any official document in which a suspicious activity or incident is recorded. In the course of conducting their missions or for the protection of their personnel and facilities, many local law enforcement agencies document suspicious activities observed or reported. This practice is well-established in the law enforcement community and occurs with varying degrees of standardization and formality in other communities as well.

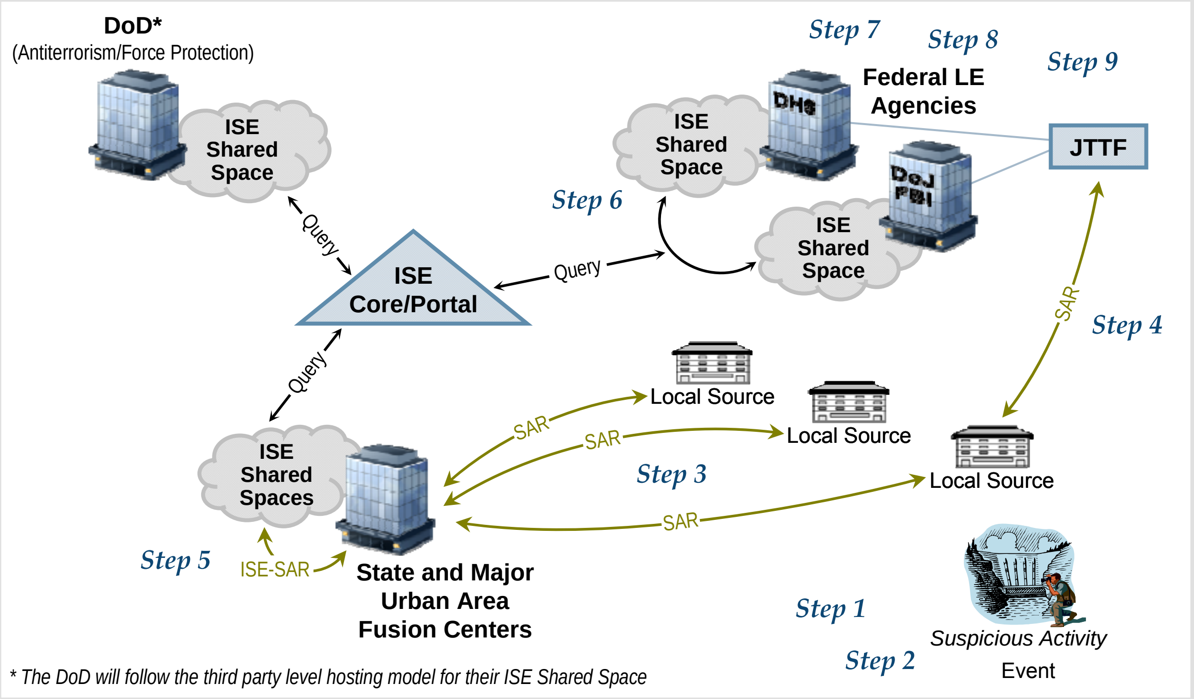
For sharing, an ISE-SAR is represented in a specific electronic format in accordance with the SAR Information Exchange Package Documentation (IEPD), which constitutes the technical artifacts of the *ISE-SAR Functional Standard.* Furthermore the detailed ISE-SAR IEPD (henceforth denoted in this Segment Architecture as the "Detailed ISE-SAR IEPD") constitutes the technical artifacts (189 element data model, data schema, and reference vocabulary) providing descriptions and relationships of all SAR data that may be exchanged, including data tagged elements (termed "privacy fields") requiring protection under privacy laws and regulations.[15] Summary ISE-SAR information (henceforth denoted in this Segment Architecture as "Summary ISE-SAR Information") is derived from the technical artifacts of the Detailed ISE-SAR IEPD, but the viewable information has the 19 privacy fields designated information stripped from any results.

Local law enforcement (LE) agencies collect and document suspicious activity information in support of their responsibilities to observe and investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. These routine activities have long been conducted in accordance with well-established local processes. Information collected generally falls into one of four categories—administrative, routine patrol function, criminal intelligence, or criminal investigative (with a criminal nexus). At the State and local levels, the use and sharing of each of these types of information are governed by department policy, local ordinances, and State laws as well as federal regulations and guidelines such as 28 Code of Federal Regulations (CFR) Part 23 and the *National Fusion Center Guidelines*.

[15] Data tagging is enabled using metadata markup technology for accessing those protected elements designated as "privacy fields" in the *ISE-SAR Functional Standard*. The Detailed ISE-SAR IEPD provides all 189 data fields that can be made available by the data owner to external users.

4.3 ISE-SAR Information Flow

The *ISE-SAR Functional Standard* describes a full nine (9) step information flow for nationwide SAR information sharing between the Federal Government and SLT partners across all five representative communities of the ISE. Figure 4-3 shows the logical SAR information flow applicable for activity in the ISE-SAR EE consistent with those activities, principles, and models standardized in the *ISE-SAR Functional Standard*. Figure 4-3 and subsequent figures identify those specific organizations, a subset of the entire ISE, that are participating in the ISE-SAR EE. The National Counterterrorism Center (NCTC), for example, is playing an indirect role in the ISE-SAR EE project; however it is part of the broader ISE-SAR process under the NSI. Detailed explanation of activities in each of the 9 steps is provided in Table 4-1. Subsequent sections in this Segment Architecture provide descriptions of portions of the 9 step information flows grouped under the ISE-SAR Top-Level business process activities, including the business process outcomes, affected services, and constraints to implement the ISE-SAR EE as logically depicted in Figure 4-3.



* The DoD will follow the third party level hosting model for their ISE Shared Space

Figure 4-3. ISE-SAR Top-level Information Flow for the ISE-SAR EE

Table 4-1. ISE-SAR Top-Level Information Flow Descriptions

(Steps from Figure 4-3 and the ISE-SAR Functional Standard)

Step	Activity	Process	Notes
1	Observation in the ISE-SAR EE	The process begins when a person or persons observe unusual behavior potentially related to terrorism. Such activities could include, but are not limited to, surveillance, photography of facilities and critical infrastructure, site breach or physical intrusion, boats anchored in atypical locations, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other usual behavior or sector-specific incidents.[16] Although this activity is part of the ISE-SAR EE, it is outside the bounds of the *ISE-SAR EE Segment Architecture* for documentation purposes.	The observer may be a private citizen, a government official, or a law enforcement or homeland security officer.
2	Initial Response and Investigation in the ISE-SAR EE	An official of a Federal, SLT agency with jurisdiction responds to the reported observation.[17] This official gathers additional facts through personal observations, interviews, and other investigative activities. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of fact-based systems to continue the investigation. These fact-based systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of fact-based systems and the information they may provide include • Department of Motor Vehicles provides drivers license and vehicle registration information • National Crime Information Center (NCIC) provides wants and warrants information, criminal history information, and access to the Terrorist Screening Center (TSC), terrorist watch list, and Violent Gang/Terrorism Organization File (VGTOF) • Other Federal, SLT systems can provide criminal checks within the immediate and surrounding jurisdictions When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).	The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports. The record may be hard and/or soft copy and does not yet constitute an ISE-SAR in the ISE-SAR EE.

[16] SAR is an official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism.

[17] If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

Step	Activity	Process	Notes
3	Local/Regional Processing in the ISE-SAR EE	The agency processes and stores the information in its RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a SLT agency or a field element of a Federal agency. SLT: Based on specific criteria or the nature of the activity observed, the SLT law enforcement components with jurisdiction would make available the information to the State or major urban area fusion center for further analysis. Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information—still only fact information—would be made available to field intelligence groups (FIGs) and/or headquarters elements through processes that vary from agency to agency. In addition to providing the fact information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.	The State or major urban area fusion center supporting the ISE-SAR EE should have access to all suspicious activity reporting in its geographic region whether collected by SLT or Federal field components.
4	Creation of an ISE-SAR	The determination of an ISE-SAR is a two-part process. First, at the supporting ISE-SAR EE State or major urban area fusion center or Federal agency, a trained analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria may have a nexus to terrorism-related activity. Once the determination is made that a potential nexus to terrorism exists, the information becomes an "ISE-SAR" and is formatted in accordance with *ISE-FS-200* (*ISE-SAR Functional Standard*). The ISE-SAR is placed into an ISE Shared Space. The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.	For SLT law enforcement, the ISE-SAR information may be classified administrative, criminal intelligence, or criminal investigative (with a criminal nexus) information handled in accordance with local codes, State laws, and/or Federal regulations. It may be shared with State or Federal law enforcement personnel with the privacy fields included (reference Section 5.1 for privacy and civil liberties protection activity).
5	ISE-SAR Sharing and Dissemination in the ISE-SAR EE	In a State or major urban area fusion center participating in the ISE-SAR EE, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative, and placed in the State or major urban area fusion center's ISE Shared Space or otherwise made available to other participants in the ISE-SAR EE. The FBI field component participating in the ISE-SAR EE enters the ISE-SAR information into the FBI designated ISE Shared Space system. The DHS representative component participating in the ISE-SAR EE enters the ISE-SAR information into the DHS designated ISE Shared Space system and sends the information to the DHS, Office of Intelligence Analysis. The DoD representative component participating in the ISE-SAR EE enters the ISE-SAR information into the third party service provider supported ISE Shared Space system.	

Step	Activity	Process	Notes
6	Federal Headquarters (HQ) Processing and Participating in the ISE-SAR EE	At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components, and incorporated into an agency-specific national threat assessment that is shared with ISE-SAR EE members.	When a State or locally originated ISE-SAR is in the Federal agency owned system, the rules of sharing are no longer governed by 28 CFR Part 23 or state or local rules of law, but rather by appropriate Federal privacy laws and guidelines.
7	NCTC Analysis	When product(s) containing the ISE-SAR information are made available to the NCTC in the ISE SAR EE, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources. NCTC has the primary responsibility within the Federal Government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site. The Interagency Threat Assessment and Coordinating Group (ITACG), housed at the NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of SLT entities and when appropriate private sector entities. The ITACG is the mechanism that facilitates the sharing of counterterrorism information with SLT.	
8	NCTC Alerts, Warnings, Notifications (Note: This description also encompasses other NCTC products in additional to Alerts, Warnings, Notifications {two specific products}).	NCTC products, informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with SLT through the State or major urban area fusion centers. The sharing with SLT and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with SLT organizations and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.	NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products shall support the information needs of SLT entities.
9	Focused Collection	The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of SLT entities and Federal field components.	

4.4 Top-Level Business Process Step: Information Acquisition

4.4.1 Description[18]

Information acquisition begins when a person or persons observes unusual or suspicious behavior that may be indicative of criminal activity associated with terrorism activity. Such activities could include, but are not limited to, surveillance, photography of facilities and critical infrastructure, site breach or physical intrusion, boats anchored in atypical locations, cyber attacks, possible testing of physical response, or other unusual behavior or a sector specific incident.[19] The observer may be a private citizen, a government official, homeland security or law enforcement officer, or other security personnel (Figure 4-4 depicts this with Step 1 of the ISE-SAR Top-Level Information Flow). The unusual activity is reported to a law enforcement (LE) agency that has jurisdiction. The LE agency responds to the report of information and may gather additional facts through personal observation, interviews, and other investigative activities. The LE official may use a number of fact-based systems, such as DMV licensing systems and the VGTOF, to continue the investigation. These fact-based systems provide the official with a more complete picture of the activity being investigated. While part of the nationwide SAR process, these activities take place outside the specific boundaries of the ISE-SAR EE being discussed here.

When the initial investigation or fact gathering is completed, the official documents the event. An official report is made and the report becomes a part of the LE agency's recording system, such as a RMS. The reporting format can be paper or electronic and will be handled in accordance with agency policy, municipal codes, State laws and Federal laws and regulations. The information is reviewed within a department by a supervisor, detective, or analyst, possibly supported by automated tools or systems, for linkages to other suspicious or criminal activity and may be categorized as administrative, criminal intelligence, or investigative information with a criminal nexus (Figure 4-4 depicts this with Step 2 of the ISE-SAR Top-Level Information Flow). This process is agency-specific, and in most cases is conducted outside the boundaries of the ISE for documentation purposes. Collection resources conform with policies to address privacy and civil liberties concerns that conform to their applicable codes, laws, and Federal regulations.

[18] Source documentation: *ISE-SAR Functional Standard, Version 1.0*.

[19] Part B of the *ISE-SAR Functional Standard* contains some general criteria for what constitutes terrorist-related suspicious activity. More specific criteria codes are included in the *Findings and Recommendations of the Suspicious Activity Report and Implementation Project*. (Final Draft, June 2008).

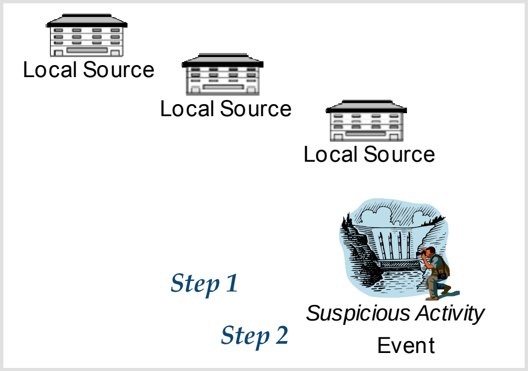


Figure 4-4. Observation and Initial Response/Investigation

4.4.2 Outcomes

None specifically prescribed through this ISE-SAR EE summary. These activities take place outside the boundaries of the ISE.

4.4.3 Affected ISE Core Service Processes

This process step of the overall business process takes place outside the boundaries of the *ISE-SAR EE Segment Architecture* for documentation purposes. The acquisition of SAR information is performed by law enforcement agencies and is governed by the business and technical architectures used by each agency.

4.4.4 Constraints

None at the present time.

4.5 Top-Level Business Process Step: Organizational Processing

4.5.1 Description[20]

Organizational processing takes place at multiple points in the overall ISE-SAR process. Once the initial information about the suspicious activity has been acquired (see Section 4.4), law enforcement agencies process and store this information in their records systems in accordance with policies and procedures that vary from one jurisdiction to another. Smaller agencies will typically forward all SARs to the State or major urban area fusion center upon completion of their internal vetting process. Although as noted above, all inputs should routinely be reviewed for linkages to other suspicious or criminal activity. Major cities, on the other hand, may have a criminal intelligence element that can apply additional analytic review of the initial reports and filter out those determined to not have a potential terrorism nexus.

Regardless of the level of processing, local agencies should provide SARs to the relevant State or major urban area fusion center.[21] Field components of Federal agencies participating in this ISE-SAR EE forward their reports to the appropriate resident, district, or division office through processes that vary from agency to agency. Alternatively organizations (for example, DoD law enforcement organizations) may input SAR data into an ISE Shared Space that is provided by a third party service provider (reference section 3.1.3 of Appendix D). This data is then available for access by other ISE-SAR EE participants including fusion centers. Federal field components may directly provide an information copy to the State or major urban area fusion center in its geographic region based on criticality. Thus, the fusion center is made aware of all suspicious activity in its area of responsibility (See Figure 4-5).

[20] Source Documentation: *ISE-SAR Functional Standard, Version 1.0*, Ibid.

[21] If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In such a case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

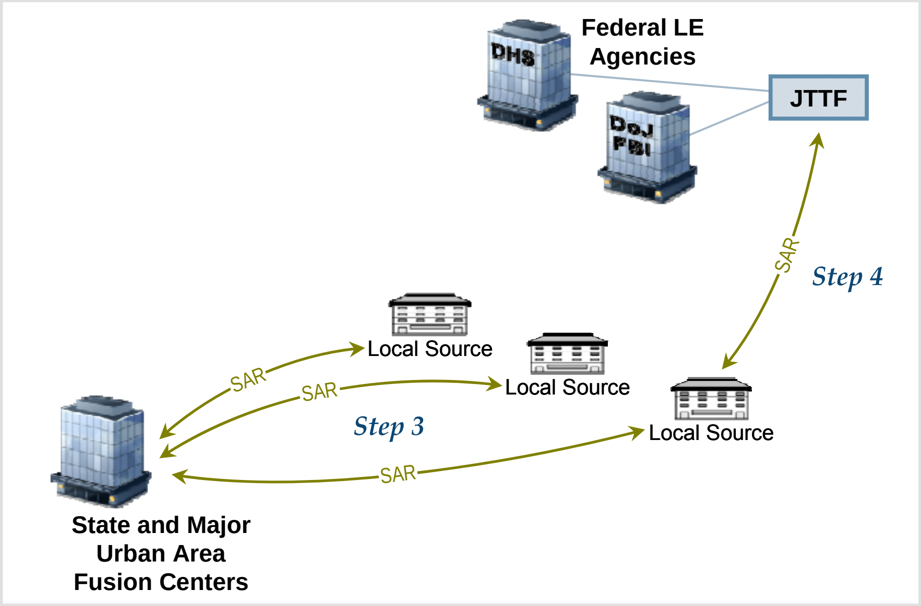


Figure 4-5. Local/Regional Processing

The fusion center or Federal agency provides an additional analytic review of all SARs received. First, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria outlined in Part B of the *ISE-SAR Functional Standard*. Second, the analyst or law enforcement officer reviews the input against all available knowledge and information for linkages to other suspicious or criminal activity, using automated tools if available. Following these activities, the officer or analyst applies professional judgment and training to determine whether the information meeting the criteria is likely to have a nexus to terrorism.[22]

If this determination is made, the information becomes an “ISE-SAR” and is formatted in accordance with the *ISE-SAR Functional Standard*.[23] This ISE-SAR is then stored in the fusion center or JTTF’s “ISE Shared Space” where it can be accessed without delay by authorized law enforcement and homeland security personnel in the State or major urban area fusion center’s area of responsibility as well as all other ISE-SAR EE participants (Figure 4-5 depicts this with Step 3 of the ISE-SAR Top-Level Information Flow).

[22] The *ISE-SAR Functional Standard* describes the determination of an ISE-SAR as a two-part process. In many cases, however, the two steps take place almost concurrently.

[23] Version 1.0 of the *ISE-SAR Functional Standard* identifies the organizations that can designate ISE-SAR as either (a) State and major urban area fusion centers or headquarters, or (b) field components of Federal Government agencies with a counterterrorism (CT) mission. One of the options to be evaluated during the ISE-SAR EE is whether or not some or all major city police departments should have similar authority.

4.5.2 Outcomes

4.5.2.1 Threshold Outcomes

- Each ISE-SAR EE participant system will make all ISE-SARs accessible to all other ISE-SAR EE participants in the Summary ISE-SAR Information format (i.e., with no privacy fields);
- Each ISE-SAR EE participant system processes SARs consistent with the *ISE-SAR Functional Standard,* ISE Privacy Guidelines, and supplementary implementation guides (reference original compliance and source documents in Section 2.5); and
- Each ISE-SAR EE participant system will be capable of accessing free-text, depersonalized (no personal information) ISE-SARs (ISE-SAR "Summary Reports") contained in the SAR Summary Reports Library.

4.5.2.2 Objective Outcome

- Each ISE-SAR EE participant system will share ISE-SARs to the applicable State and major urban area Fusion Center in the Detailed ISE-SAR IEPD format of the *ISE-SAR Functional Standard* and with all other ISE-SAR EE participants to the maximum extent permitted by its laws, regulations, and policies. This is contingent on meeting privacy requirements documented in Section 5.1.

4.5.3 Affected ISE Core Service Processes

- The *Mediation and Storage* service processes, as described in the *ISE EAF*, support the Organizational Processing phase of the ISE-SAR process.

4.5.4 Constraints

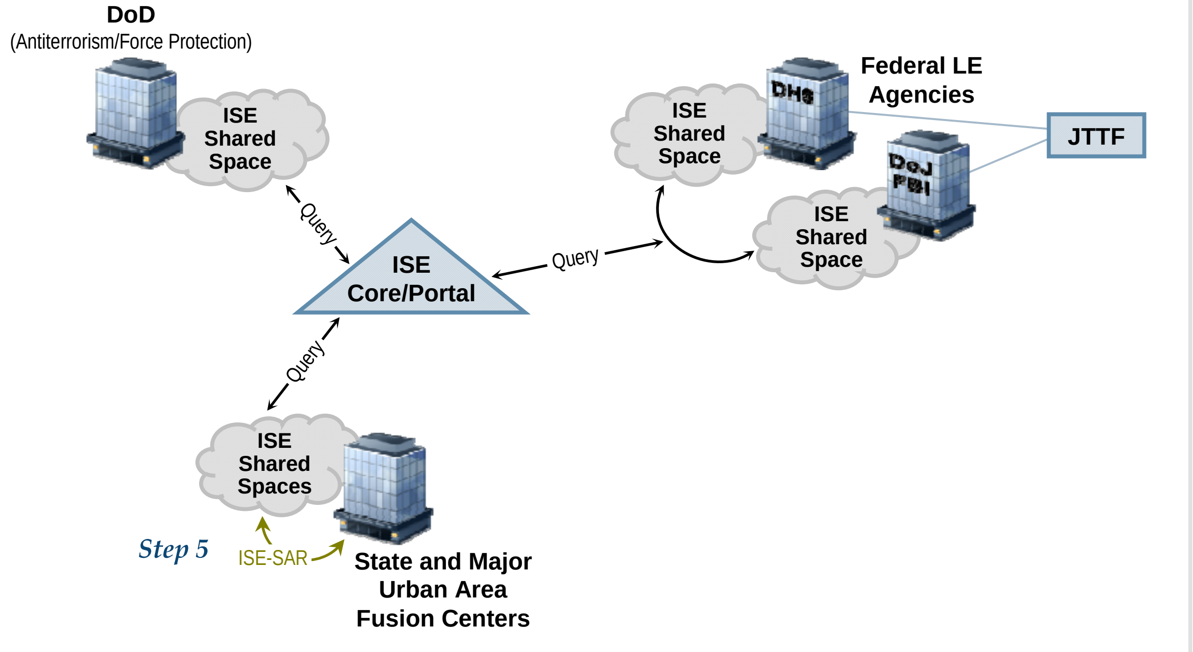
None noted at this time.

4.6 Top-Level Business Process Step: Integration/Consolidation

4.6.1 Description[24]

The Integration/Consolidation phase of ISE-SAR EE implementation involves making the individual ISE-SAR EE participant's SAR information available for searching across the ISE-SAR EE. This integration includes supporting data mapping and translation in internal databases, as appropriate, to aid with local control of data[25]. The ISE-SAR EE has been extended to interface up to 12 sites, additional data sources, and more hardware/network interfaces (see Figure 4-6).

Once the determination is made that the suspicious activity has a potential terrorism nexus, the information becomes an "ISE-SAR" and is formatted in accordance with the *ISE-SAR Functional Standard*. This ISE-SAR is then stored in the fusion center or JTTF's associated "ISE Shared Space" where it can be accessed by authorized law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility as well as by all other ISE-SAR EE participants (Figure 4-6 depicts this with Step 5 of the ISE-SAR Top-Level Information Flow).



* The DoD will follow the third party level hosting model for their ISE Shared Space

Figure 4-6. Creation, Sharing, and Dissemination of an ISE-SAR

[24] Source Documentation: *ISE-SAR Functional Standard, Version 1.0*; *ISE EAF, Version 2.0*; SAR Proposal for Continuation and Expansion of National SAR Implementation and Regional SAR Analytical Collaboration Capabilities.

[25] For purposes of this ISE-SAR EE, "local control" refers to control by the organization that generated the initial SAR report.

4.6.2 Outcomes

4.6.2.1 Threshold Outcomes

From a threshold outcomes perspective, the integration/consolidation activity in the ISE-SAR EE requires:

- Each ISE-SAR EE participant system processes and stores all ISE-SARs in their ISE Shared Space consistent with the *ISE-SAR Functional Standard*, ISE Privacy Guidelines, and supplementary implementation guides (reference original compliance and source documents in Section 2.5);
- ISE-SAR EE sites may store Detailed ISE-SAR IEPDs in their ISE Shared Spaces if they meet the reasonable suspicion threshold, however they must also demonstrate that the necessary privacy and civil liberties policy framework is in place, both at their site and the viewing site(s), in order to share Detailed ISE-SAR IEPD records. If the necessary policy framework is not in place at the ISE-SAR EE site and the viewing site(s), only Summary ISE-SAR Information formatted records (exclusive of personal information) may be shared from the respective ISE Shared Space;
- Each ISE-SAR EE participant manages and maintains the ISE-SARs submitted to its ISE Shared Space. The owner of the ISE Shared Space may not in all cases be the source originator of the SAR data. In addition, the same incident or suspicious behavior may be reported by more than one organization;
- ISE-SAR data in ISE Shared Spaces is available for search and viewing to all the approved users of the ISE-SAR EE; and
- Only the ISE-SAR EE participant managing an ISE Shared Space, or the originator of the ISE-SAR, may update/modify/delete the ISE-SARs hosted in that ISE Shared Space.

4.6.2.2 Objective Outcomes

No objective outcomes for this business process step. All outcomes for this Top-Level business process step are threshold.

4.6.3 Affected ISE Core Service Processes

The *Mediation* and *Storage* service processes, as described in the *ISE EAF*, support the Integration/Consolidation phase of the ISE-SAR process.

4.6.4 Constraints

An ISE-SAR EE participant must maintain and control security permissions and permit outside users (other authorized ISE-SAR EE participants) access to ISE-SAR data in the ISE Shared Space(s) via a protected CUI/SBU connection. Security must be maintained at an appropriate level (i.e., CUI is the operational security domain for the ISE-SAR EE). Uploaded data must comply with policy guidelines (protecting privacy and civil liberties), and data formats from the *ISE-SAR Functional Standard*. The “Dissemination Code” field in the *ISE-SAR Functional Standard* is used for verifying, from the ISE-SAR originator, whether the information stored should not be disseminated, or should be checked before dissemination to other ISE-SAR participants.

4.7 Top-Level Business Process Step: Data Retrieval/Distribution (Data will be View Only)

4.7.1 Description[26]

A critical component of information sharing is the ability to search for needed information and view that information on the requestor's desktop computer. It is important to note that data will be visible to authorized users but will reside only in the originating organization's designated ISE Shared Space. As documented in the *ISE-SAR Functional Standard*, the SAR Retrieval/Distribution business process begins when a requestor initiates a request for information from the ISE-SAR EE and is completed once that information is viewable by the requestor. This process requires the ability to build queries, conduct federated searches, consolidate and display results, and view records (see Figure 4-7).

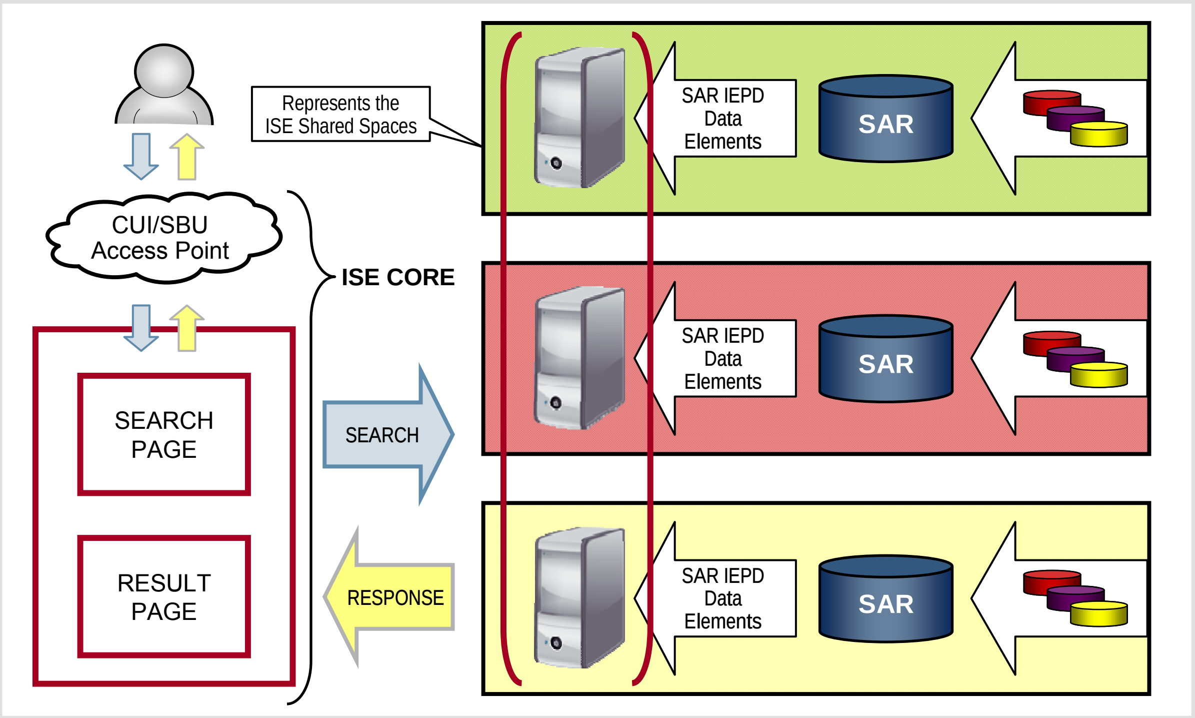
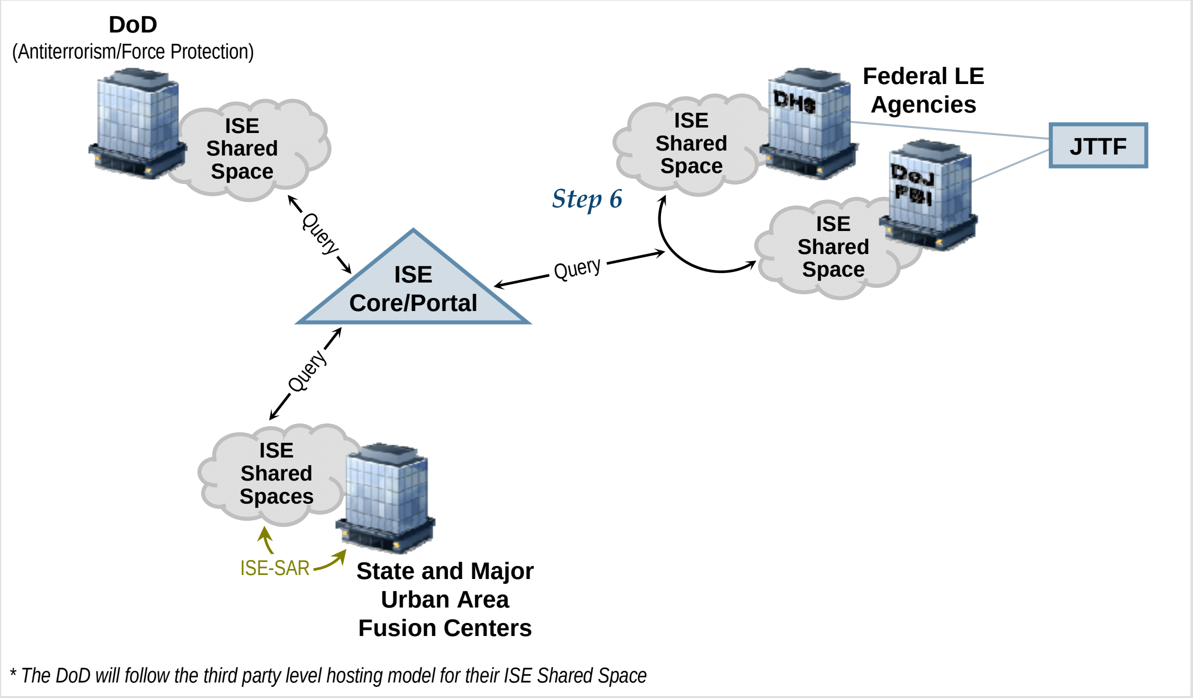


Figure 4-7. ISE-SAR Retrieval and Distribution

[26] Source Documentation: SAR: Proposal for Continuation and Expansion of National SAR Implementation and Regional SAR Analytical Collaboration Capabilities, (Bureau of Justice Assistance, May 2008); PM-ISE/BJA Memorandum of Agreement (29 July 2008); *ISE EAF, Version 2.0*, September 2008; *ISE-FS-200: ISE Functional Standard (Suspicious Activity Reporting), Version 1.0.*

A search may consist of a single-site area search for free-text records in the SAR Summary Reports Library, or across all relevant (participating) ISE Shared Spaces, or it may be pointed toward a select subset of a particular ISE Shared Space. The search is based on a select set of parameters from the *ISE-SAR Functional Standard* and associated IEPD artifacts. The results of the search should, at a minimum, include sufficient information to give the user a reasonable understanding of the content of the record. The user should then be able to select from the initial set of search results to view the record. For purposes of this ISE-SAR EE, the SAR distribution process is limited to viewing the records on-screen (Figure 4-8 depicts this with Step 6 of the ISE-SAR Top-Level Information Flow).

For auditing purposes, the search capability should collect data on the requestor (authorizations, permissions), justification for the search, time and date of the search, and the specific search query.



* The DoD will follow the third party level hosting model for their ISE Shared Space

Figure 4-8. Federal HQ Processing

4.7.2 Outcomes

ISE-SAR information is useful only to the extent that it can be found and used by the ISE-SAR EE participant community. Because of the sensitive nature and potential for abuse of personal information captured in ISE-SARs, restrictions on access to/dissemination of personal information must be applied. These restrictions are reflected in the following Threshold and Objective Outcomes.

4.7.2.1 Threshold Outcomes

The ISE-SAR EE is limited in size and scope. The ISE-SAR EE will not demonstrate full operational capability to the entire ISE as envisioned for the future, only to those participating organizations identified in Section 2.2. Information sharing among approved ISE-SAR EE participants is a minimum (threshold) objective. Success will be achieved when the following are demonstrated:

- Search Participating ISE Shared Spaces in the ISE-SAR EE
  - Authentication for access and search will be controlled consistent with guidance from the ISE Identity and Access Management (IdAM) Framework [documented in the ISE EAF, Version 2.0 and ISE Guidance (G)-108] and the Technical Standard: Information Assurance (ISE-G-106)[27].
- Identify and View Relevant Information from the SAR Summary Reports Library and ISE Shared Spaces
  - The search capability displays results from "Summary Reports" within the SAR Summary Reports Library, based on unstructured text searches;
  - The search capability displays results drawn from ISE Shared Spaces participating in the ISE-SAR EE; and
  - The information is displayed accurately and completely reflects the data in the ISE Shared Spaces.
- In conducting the search function across ISE Shared Spaces, inadvertent or unauthorized release of sensitive and/or personal information must be prevented
  - *Protect Personal Information from Unauthorized Access:* Personal information within the ISE Shared Spaces shall be protected, consistent with public law and policy governing protection of personal information; and
  - *Provide Audit Tracking:* The search capability shall log information about the organization of the originator of the search, including the originator's authorization or permissions, the justification for the search, the time and date of the search, and an optional reference number field will also be provided[28].

4.7.2.2 Objective Outcomes

The purpose of sharing ISE-SAR information is to ensure the analysis and integration of information leading to the disruption of terrorist activities. The objective of the search functionality for an authorized member of the ISE-SAR EE is to successfully find ISE-SAR-related data in any participating ISE Shared Space.

- Search Participating ISE Shared Spaces – ISE-SAR data in participating ISE Shared Spaces should be accessible and searchable through an integrated, federated process. The search capability should be able to identify needed information through flexible queries. This tool should allow a user to find known data as well as to discover information previously unknown to the requestor.

[27] These technical standards are available from PM-ISE or may be downloaded at www.ise.gov.

[28] Reference the *NSI CONOPS, Version 1.0* for description of this activity.

  - ◦ *Search/Query Participating ISE Shared Spaces:* The search capability must be able to query participating ISE Shared Spaces. ISE Shared Spaces will be configured to use an internal search process. The federated search function must accommodate internal search capability to query the database and receive the resulting information;
  - ◦ *Selectively Query ISE Shared Spaces:* The tool should be capable of searching or querying one or more selected ISE Shared Spaces as well as performing broad area searches of all relevant ISE Shared Spaces;
  - ◦ *Search Unstructured/Semi-Structured (Non-database) Data in the SAR Summary Reports Library:* Some data are in non-database formats, (e.g., documents, reports, various free text formats). There must be a search capability to conduct word searches in such formats;
  - ◦ *Maintain Maximum Availability:* The search tool should be useable across a broad spectrum of users participating in the ISE-SAR EE;
  - ◦ *Integrate Results (Federated Search):* The search tools should be capable of providing a consolidated presentation of the search results, be they from a single ISE Shared Space or the results of queries from multiple ISE Shared Spaces; and
  - ◦ *Enable Data Screening or Preview:* The initial results list shall display submitting organization, contact information, and information sought. The search capability should be able to sort the initial search results based on the categories of information displayed.
- Display needed data from participating ISE Shared Spaces – Once found, the information should be viewable from participants' ISE Shared Spaces by any authorized requestor.
  - ◦ *View Information:* An authorized user should be able to view all ISE-SAR data responsive to the query that exists in participating ISE Shared Spaces subject to established limits on the number of records that can be accessed in response to an inquiry;
  - ◦ *Accurately Display Information:* The search results must accurately reflect the data extant in the ISE Shared Spaces, displayed without unintended alteration or introduced errors on the user's desktop computer; and
  - ◦ *Failed Contact Indicator:* The search capability should indicate any failures to access ISE Shared Spaces.

4.7.3 Affected ISE Core Service Processes

Discovery – Discovery provides a way for the ISE-SAR EE participant to search federated search-enabled data sources via the ISE Portal concept demonstrated in the ISE-SAR EE.

Security – Security services provide protection mechanisms to the participants in the ISE-SAR EE through support of control processes. This functional service would provide the necessary protections for controlling accesses to ISE Shared Spaces and the stored information. Systems must ensure information protection consistent with relevant guidelines.

Mediation – Data and services must be stored in a location and manner accessible to and compatible with the search tool. Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchanges between data producers and consumers. Mediation Services include data transformation and adaptation. Mediation may not be required if there exists a commonality of hardware or software; however, in the case of the ISE-SAR EE, this service would accommodate the interfacing of disparate ISE-SAR EE participants' systems.

Enterprise Service Management (ESM) – ESM functionality is the continuous process of managing, measuring, reporting, and improving the quality of service of ISE-SAR EE systems and applications. ESM monitoring and status alerts will provide ISE-SAR EE participants with notifications of failures to access any ISE Shared Spaces.

Storage – Storage services would include capabilities to achieve content search and delivery via ISE Shared Spaces. This process would be applicable to the storage of information according to the data formats outlined in the *ISE-SAR Functional Standard*.

Collaboration – Collaboration enables communication and viewing among participants via the ISE-SAR EE. Collaboration uses a full range of accessible, hosted, managed, and content storage services, involving various levels of interaction. Collaboration enables ISE-SAR EE participants to discover and interact directly with other ISE-SAR EE participants.

4.7.4 Constraints

ISE-SAR Data Formats – While information in the SAR Summary Reports Library may be found in many forms and formats (ranging from documents to briefing slides, memos and e-mails), data in ISE Shared Spaces conforming to the *ISE-SAR Functional Standard* are more easily searched, sorted, and viewed.

Search Tool Interface – A federated search tool will interface with each ISE Shared Space-internal search/query tool. This constraint would require the federated search tool to have the ability to translate/pass queries to a database search/query service within a targeted ISE Shared Space.

Preventing Unauthorized Release of Personal Information – In the course of providing search results, the search tool should not reveal personal information to a user not authorized to receive such data.

Leveraging Existing Systems, as practicable – Section 1016(b)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, directs that the sharing of terrorism information through the ISE be done in a manner that leverages existing systems to the greatest extent practicable. While no single system or database exists, the search, retrieval, and distribution functionality in the ISE-SAR EE should leverage existing capabilities, infrastructures, and services where appropriate.

4.8 Top-Level Business Process Step: Feedback

4.8.1 Description[29]

A feedback loop has been an integral part of the ISE-SAR business process and the *ISE-SAR Functional Standard*. It was recognized early that feedback to collectors and analysts on the value of their contributions was an important element of an integrated ISE-SAR EE strategy.

The SAR Business Process Analysis (BPA) recognized the need for three different types of feedback:

- Administrative feedback regarding possible future process modifications, e.g., updates to the *ISE-SAR Functional Standard*, lessons learned from earlier pilot efforts, and from the ISE-SAR EE, etc.
- Operational feedback to ISE participants regarding the disposition of ISE-SARs; and
- Crossflow/Backflow (Collaborative activities).

The requirement for administrative feedback should be met through a number of methods that are both qualitative and quantitative and can be collected via system usage statistics, and analysis of data at individual agencies, and in ISE Shared Spaces.

In operational terms, feedback is provided to originating agencies when/if a submitted SAR becomes an ISE-SAR or when an ISE-SAR is found to have been designated in error. The ISE-SAR EE participant has the responsibility to provide feedback to a submitting organization. This process essentially takes place when the ISE-SAR EE participant determines or receives information that the SAR was erroneously designated an ISE-SAR or that an ISE-SAR contains erroneous information.

4.8.2 Outcomes

In general, the overall objective outcome is to improve the Federal Government's efforts to develop an integrated plan and provide State and major urban area fusion centers a mechanism to gather and report locally generated information to appropriate Federal entities, other States, and localities. This locally generated information will include reports by the public or governmental personnel to law enforcement agencies regarding suspicious incidents, events, and activities.[30] Each of these goals requires that an effective Feedback mechanism be in place and used by all ISE-SAR EE participants.

4.8.2.1 Threshold Outcomes

The ISE-SAR EE will be of limited size and scope involving only selected Federal agencies, and up to twelve State or major urban area fusion centers identified in Section 2.2. As such, it may not be able to demonstrate full capability of feedback objective outcomes across the entire

[29] Source Documentation: Draft Phase 1 Evaluation Plan (BJA), Draft Phase 1 Interim Report Outline (BJA).

[30] White House, *National Strategy for Information Sharing*, Ibid., A1-6.

planned ISE. Information sharing among ISE-SAR EE participants is a minimum (threshold) objective. Success will be achieved when the following are demonstrated:

- ISE-SAR EE participant systems continually measure and verify that the *ISE-SAR Functional Standard* effectively meets the needs of law enforcement agencies.
    - Examine the capabilities of the automated ISE-SAR collection and reporting systems currently used by ISE-SAR EE participants to identify areas of commonality and gaps when compared to the *ISE-SAR Functional Standard* elements;
    - Evaluate whether ISE-SARs contributed to the SAR Summary Reports Library or made available to a participant's ISE Shared Space conform to the ISE-SAR criteria specified in the *ISE-SAR Functional Standard;*
    - Measure the effectiveness of search tools in retrieving ISE-SAR data based upon unstructured search parameters in either ISE Shared Spaces or the SAR Summary Reports Library;
    - Measure the usage of the ISE-SAR EE over the evaluation period; and
    - Provide mechanism(s) to alert participants when an ISE-SAR is found to have been designated in error.

4.8.2.2 Objective Outcomes

Specific objective outcomes for the Feedback service in the ISE-SAR EE include

- ISE-SAR EE participants' measure and verify that the *ISE-SAR Functional Standard* (ISE-SAR designation criteria and information formats) meets the needs of law enforcement agencies and that user feedback informs required version updates to the *ISE-SAR Functional Standard* to reflect the needs of the law enforcement community and the ISE. The following high-level sub-objectives are planned:
    - Based on the ISE-SAR EE, verify the *ISE-SAR Functional Standard* criteria for completeness and usefulness in a multi-agency Federal, and SLT user base;
    - Follow the governance framework described in ISE-SAR EE and ISE documentation to ensure that common definitions of suspicious behavior identified by participating agencies are codified and implemented to the greatest extent possible; and
    - Based on the ISE Shared Spaces model, examine the *ISE-SAR Functional Standard* to ensure that the ISE-SAR data model in the IEPD component fully captures desired information sharing components and is consistent with on-going Law Enforcement Information Sharing Program Exchange Specifications (LEXS) and/or National Information Exchange Model (NIEM)/Universal Core(UCORE)[31] initiatives.
- Establish appropriate capabilities in systems to improve collaboration between investigators and analysts in multiple agencies to
    - Improve situational awareness within the law enforcement community and private sector;
    - Link disparate investigations or incidents to common SAR activity; and
    - Solve or interdict criminal activities with potential terrorist connections.

[31] Reference the *ISE EAF, Version 2.0* (Section 7.3.1) for details on NIEM and UCORE alignment efforts.

- Establish the systems' capabilities for law enforcement agency investigators and analysts to identify best practices, lessons learned, or success stories with ISE-SAR EE systems that the participants and other members of the ISE-SAR EE may choose to adopt.
- Establish appropriate capabilities in ISE-SAR EE systems for improving collaboration between investigators and analysts in multiple agencies to
  - Provide mechanisms to deliver feedback to originating agencies, when/if a submitted SAR becomes an ISE-SAR;
  - Measure the comparative frequency of ISE-SAR EE participants' submissions to the SAR Summary Reports Library and to ISE Shared Spaces; and
  - Establish survey tools, user groups, or on-line interview process capabilities to solicit end-user feedback on whether the ISE-SAR EE systems helped analysts create new cases, link previous disparate cases or incidents, or helped solve or interdict potential terrorism-based crimes or activities.
- Establish the systems' capabilities for law enforcement agency investigators and analysts to identify best practices, lessons learned, or success stories and share that information within the law enforcement community.
  - Establish an on-line repository for end-users to contribute best practices, lessons learned, and success stories that may assist investigators and analysts in identifying and interdicting terrorist activities.

4.8.3 Affected ISE Core Service Processes

Discovery – The ability for an authorized ISE-SAR EE participant to search the SAR Summary Reports Library or ISE Shared Spaces for information on a particular incident, suspicious activity, location, or other search parameters and have the results of the search returned to the user's browser for viewing. Search results should also be structured based on the *ISE-SAR Functional Standard* so that such results could also be processed by other applications used by the analyst in the future. This includes the ability to push selected SAR records from an ISE-SAR EE participant's existing legacy system to an ISE Shared Space on a periodic basis when such SARs meet the ISE-SAR standard criteria.

Enterprise Service Management – The ability of the investigator or analyst to access desired ISE-SAR data from various secure system resources.

4.8.4 Constraints

The primary constraint to achieving the outcomes and objectives described earlier in this section, as with the ISE-SAR EE in general, is the availability of sufficient ISE-SAR data of interest to the end-user during search operations against the SAR Summary Reports Library or the ISE Shared Spaces environment. This constraint may exist for several reasons. Because the ISE-SAR EE sites are geographically dispersed, there may be little data commonality between the existing sets of ISE-SAR reports. Second, the legacy SAR reports or data records contributed by ISE-SAR EE participants may not follow any particular standards in the way information is coded or expressed in narrative fields. Third, because of privacy and or civil liberty concerns, certain agencies may be unwilling to share detailed data with all ISE-SAR EE participants. While this decision may not inhibit investigative or collaboration activities resulting from the analysis of search results, the timeliness of such activities could be affected.

5 ISE-SAR EE Enabling Services to Support EE Outcomes

ISE-SAR EE enabling services constitute those generalized services required for implementation and use throughout the ISE-SAR EE. These services are effected through procedural, operational, and technical implementation efforts at and between ISE-SAR EE sites and with their representative IT systems. The ISE-SAR EE enabling services include privacy and civil liberties protection, access, information assurance, resource/network management, and trending/analysis. The following sections describe these enabling services in detail, identify threshold and objective outcomes, identify those related ISE Core Service processes from the ISE architecture, and identify pertinent constraints.

5.1 Privacy and Civil Liberties Protection

A goal for the ISE-SAR EE, and ultimately for the ISE generally, is for ISE-SARs to be shared, to the maximum extent possible, among SLT and Federal law enforcement, homeland security, and other appropriate organizations participating in the ISE, while protecting privacy and other legal rights.

5.1.1 Description[32]

Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA), calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, provides that, "[to] the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies … [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …." The Privacy Guidelines apply to information about United States citizens and lawful permanent residents that are subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the Intelligence Community (IC), protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, and should be covered by the Privacy Guidelines.

The *ISE-SAR Functional Standard* is intended to support broad dissemination of ISE-SARs and sharing of the maximum relevant information in order to protect privacy and other legal rights. As described in Section 4.2, to facilitate this dissemination/access (sharing), two different formats from the *ISE-SAR Functional Standard* are available for ISE-SAR information. The **Detailed ISE-SAR IEPD** format includes personal information contained in the data fields set forth in Section IV of the *ISE-SAR Functional Standard* ("ISE-SAR Exchange Data Model"),

[32] Source Documentation: *Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect Americans*, Ibid.; *ISE-SAR Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis*, Ibid.; *ISE Privacy Guidelines*, Ibid.; *Privacy and Civil Liberties Implementation Guide for the ISE, Version 1.0*, Ibid.; *Protecting Civil Rights: A Leadership Guide for State, Local, and Tribal Law Enforcement*, Ibid.; Global *Guide to Conducting Privacy Impact Assessments for State and Local Information Sharing Initiatives* (DRAFT), Ibid.; *Guidance Regarding the Use of Race in Law Enforcement Agencies*, Ibid.

including “privacy fields” denoted as containing personal information. If an ISE-SAR EE participant is not authorized to disseminate personal information from a particular ISE Shared Space (e.g., the requester site does not have a compliant privacy policy) or the SAR does not evidence the necessary nexus to terrorism-related crime as required by the *ISE-SAR Functional Standard*, information from the privacy fields will not be loaded into the responsive document (search results) in the ISE Shared Space, and therefore will not be passed to the ISE-SAR EE participant. The **Summary ISE-SAR Information** format *excludes* privacy fields or data elements identified in Section IV of the *ISE SAR Functional Standard* as containing personal information.

5.1.2 Outcomes

5.1.2.1 Threshold

From a threshold outcomes perspective, the following is required:

- ISE-SAR EE mechanisms (procedural, operational and technical) will ensure that Detailed ISE-SAR IEPDs (ISE-SARs with personal information) do not violate civil rights and civil liberties, and that they adhere to policies regarding, for example, First Amendment protections or those that prohibit racial, ethnic, or religious profiling; and
- ISE-SAR EE sites may store Detailed ISE-SAR IEPDs in their ISE Shared Spaces if the site possesses the appropriate privacy and civil liberties policy framework and the SARs meet the requirement of the *ISE-SAR Functional Standard* to have a potential nexus with terrorism-related criminal activity. In addition, in order to share Detailed ISE-SAR IEPD records, the EE sites also must demonstrate that the viewing site has implemented the necessary privacy and civil liberties policy framework. Absent the necessary policy framework at the ISE-SAR EE site and the viewing site(s), only Summary ISE-SAR Information formatted records (exclusive of personal information) may be shared from the submitting agency’s ISE Shared Space.

5.1.2.2 Objective

Specific objective outcomes for privacy and civil liberties in the ISE-SAR EE are as follows:

- Non-Federal ISE-SAR EE participants will develop and implement privacy policies that afford privacy and civil liberties protections at least as comprehensive as those developed for Federal entities under the ISE Privacy Guidelines; and
- Federal ISE-SAR EE participants that disseminate or retrieve ISE-SARs using the Detailed ISE-SAR IEPD will ensure that data in ISE-SAR systems/ISE Shared Spaces is protected consistent with an ISE-Privacy Guidelines-compliant privacy policy.

5.1.3 Affected ISE Core Service Processes

In addition to personnel training, a number of ISE Core service processes used in the ISE-SAR EE will support and assist the ISE-SAR EE users and their IT systems in achieving privacy and civil liberties protections. These are

Mediation – In order for documentation of suspicious activity to be considered an ISE-SAR under the *ISE-SAR Functional Standard,* it must relate to the crime of terrorism and involve subjects whose potential involvement in that activity cannot be discounted. Only SARs meeting these standards will be designated an ISE-SAR and be formatted in the manner prescribed by the *ISE-SAR Functional Standard*. The data fields coded as privacy fields in the *ISE-SAR Functional Standard* are the minimum data that all jurisdictions likely consider to be privacy protected, although each ISE-SAR submitting agency can exclude additional data elements from the Summary ISE-SAR Information format in accordance with its own legal and policy requirements. Mediation services will provide for interoperability and adaption of these different formats.

Collaboration – For the ISE-SAR EE, the submitting organizations store ISE-SARs in dedicated locations (ISE Shared Spaces). In the near term, the submitting organization will determine the system into which the ISE-SAR will be entered, and the business rules governing access for that system will determine who can access it. Periodically, ISE-SARs stored in the ISE-SAR EE participants' designated SAR records management system will be transferred to its ISE Shared Space and made available to the broader ISE-SAR EE community through federated identity management capabilities. The expectation is that such systems would enable the maximum possible sharing across the ISE. Long term, the intent is to establish an ISE-wide system of attribute-based access controls that would manage access authorization based on the class or operational role of the ISE-SAR EE participant requesting access. Under such a system, it would be possible, for example, to grant full access (including privacy fields) to one set of users, where such users have a need for such fields, partial access (entire ISE-SAR minus privacy fields), or, in some cases, no access. Realization of this goal will require the development and issuance of common access standards and requirements across the ISE. The submitting organization will ensure that its own ISE Shared Space effectuates applicable privacy protections with respect to access to information contained in the privacy fields.

In the ISE-SAR EE, Detailed ISE-SAR IEPD information (i.e., including personal information in a designated privacy field) may be available to all credentialed participants possessing access to designated CUI networks. These systems will support vetting of members prior to granting access to information. Depending on the network selected, access may be limited to those with law enforcement responsibilities or functions.

These expectations for sharing reflect the mandate of Executive Order 13388, which requires that Federal "agencies give the highest priority to … the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities … [and directs that] the head of each agency that possesses or acquires terrorism information … shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency unless otherwise directed by the President or precluded by law."

Of equal weight, however, is the requirement to "protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …" Thus operationally, the expectation is to share non-privacy related ISE-SAR information to the maximum extent in ISE-SAR EE participant systems through the Summary ISE-SAR Information format, while making available the Detailed ISE-SAR IEPD where appropriate and necessary, and subject to legal and policy limits.

Discovery – Pending adoption of appropriate ISE-SAR privacy policies, the ISE-SAR EE sites that are testing the *ISE-SAR Functional Standard* will share only Summary ISE-SAR Information formatted records (no personal information) from their particular ISE Shared Spaces. Ultimately, upon implementation of policy protections, ISE participants in the ISE-SAR EE may retrieve either the Detailed ISE-SAR IEPD records (i.e., including personal information) or only the Summary ISE-SAR Information, as appropriate, depending on roles, authorizations, and demonstrated need for personal information. Initially, however, the ISE-SAR EE sites will disclose detailed privacy elements only through individualized contact with and justification of need by the requester.

The initial ISE-SAR EE architecture and *NSI CONOPS* limit retrieval from ISE-SAR EE sites to "view only" access. In the future, should users access and incorporate ISE-SARs into their own systems, a full examination of the applicable business rules and policies shall be undertaken. Central to that examination is whether, to what extent, and through what mechanism(s) the policies and practices of the submitting organization (e.g., purge dates, dissemination limitations) continue in effect for ISE-SARs received into the user's system.

The *ISE-SAR Functional Standard* presumes that ISE-SAR information may be retrieved using a variety of search keys, including personal identifiers, in the case that a user has appropriate access to Detailed ISE-SAR IEPD. Using a personal identifier as the search key results in a more narrowly focused set of search results than would broader categories such as geographic area. Federal entities administering their ISE-SARs by personal identifier must comply with the requirements of the Privacy Act to establish a Privacy Act System of Records Notice. Searches of Summary ISE-SAR Information format records would not be based on personal identifier.

Storage – Each government entity that obtains and documents information concerning suspicious activities at the Federal, SLT level must retain such information in accordance with applicable law and policy. Retention limits can vary significantly across ISE-SAR EE participant organizations and may depend upon the type of information contained in the ISE-SAR. Rather than impose a single retention standard for all ISE-SARs, the *ISE-SAR Functional Standard* allows submitting organizations to manage retention (control) of ISE-SARs within their own ISE Shared Space. Accordingly, the *ISE-SAR Functional Standard* includes the Privacy Purge Date and the Privacy Purge Review Date fields that allow the submitting organizations to "tag" protected information with "purge" or "review" (and "purge if not validated") dates. The analyst's determination to extend the report purge date must consider the continued value of the privacy elements in light of policies limiting retention of sensitive protected information by law enforcement entities. Each submitting organization's ISE Shared Space will be enabled to facilitate the timely review and/or purge of data and to permit submitting organizations to "recalibrate" purge and review dates as appropriate. The storage core service also enables systems to store and deliver data in ISE Shared Spaces in the various formats contemplated by the *ISE-SAR Functional Standard* and the ISE-SAR EE (i.e., the Summary ISE-SAR Information, Detailed ISE-SAR IEPD formats if policy frameworks are in place and the SAR meets the terrorism nexus requirement of the *ISE-SAR Functional Standard*, and the free-text SAR Summary Reports from the SAR Summary Reports Library).

Security – Security services provide confidentiality, integrity, and availability of data and associated systems for ISE-SAR EE participants. The *ISE-SAR Functional Standard* standardizes the format and content of an ISE-SAR but does not address the auditing and technical safeguards applicable to agencies' SAR systems or ISE Shared Spaces. These safeguards and procedures, such as retention of log data and frequency of audits, will vary from state to state, agency to agency, and department to department. Accordingly, non-federal ISE-SAR EE sites will establish and implement auditing and technical safeguards that are at least as comprehensive as those required by the ISE Privacy Guidelines. ISE-SAR EE participants' systems will safeguard data using appropriate authentication, authorization and access controls. Systems utilized in the ISE-SAR EE initiative must ensure information protection consistent with NIST, DOD, and National Fusion Center guidelines.

Additionally, all searches will be logged so as to identify the user's organization, and to record the user's authorizations/permissions, the search conducted and the justification for the search. The time and date of the searches will also be documented. The logging function enables supervisory personnel to identify questionable uses of the search tool and take appropriate measures.

5.1.4 Constraints

The constraint on the implementation of the *ISE-SAR Functional Standard* is whether or not the ISE-SAR EE sites delay in developing and implementing their privacy and civil liberties policies. Before sharing the Detailed ISE-SAR IEPD, ISE-SAR EE sites will implement robust privacy and civil liberties policies consistent with the ISE Privacy Guidelines and with the recommendations articulated in the Functional Standard Privacy and Civil Liberties Analysis. Where relevant, ISE-SAR EE sites will obtain participation agreements from source agencies in order that privacy and civil liberties safeguards apply at the initial reporting stages.

5.2 Access

Based on the requirements set forth in the *National Strategy for Information Sharing*, in order for terrorism information sharing to take place, a common and collaborative access process and Identity and Access Management (IdAM) standard is required.

5.2.1 Description[33]

Access may be generally defined as the "process used to grant an individual access to information and associated resources of ISE member communities based on verification of the individual's identity and associated attributes."[34] For this ISE-SAR EE, access services will be focused on those ISE Shared Spaces that are associated with primary participants of the ISE-SAR EE and their corresponding ISE-SAR data. Such ISE-SAR information will be safeguarded in accordance with applicable laws, rules, policies, and practices.

Access services are provided by core private networks in which each ISE Shared Space resides using a federated identity and access management approach for approved ISE-SAR EE participants. Once an ISE-SAR EE user has been processed through the home network's access credentialing system, the authorized user will have access to the various ISE Shared

[33] Source Documentation: *Nationwide Suspicious Activity Reporting Initiative: Concept of Operations*, Ibid.; *ISE-G-108* (Identity and Access Management Framework for the ISE, Version 1.0); *ISE Enterprise Architecture Framework, Version 2.0*; PM-ISE/BJA Memorandum of Agreement (MOA), 29 July 2008.

[34] General ISE Access definition, ISE Business Process Working Group (BPWG), March 27, 2007.

Spaces through a local access control list that is demonstrated as part of the demonstrated ISE Portal concept. These core networks satisfy the four access control capabilities required for the ISE-SAR EE: **identity** describing the set of physical and behavioral characteristics, as appropriate, by which an ISE-SAR EE user is uniquely recognizable; **confidentiality** using common methods for protecting credentials that include encryption, limited caching, and frequent refreshing; **authentication** to verify the identity of an ISE-SAR EE user as a prerequisite to permitting initial access to ISE Shared Spaces in the ISE-SAR EE; and **access**, in general, matching the attributes of structured, tagged data in the ISE Shared Spaces with uniquely tailored user attributes.

5.2.2 Outcomes

In general, the outcomes for this focus area are to grant access to ISE Shared Spaces and ISE SAR data to all authorized participants in the ISE-SAR EE project while ensuring the confidentiality, integrity, and availability of the subject data and related systems.

5.2.2.1 Threshold Outcomes

From a threshold outcome perspective, the Access service in the ISE-SAR EE must ensure

- Security of identity credentialing and access control to shared terrorism information;
- Currency of identity credentialing and access control to shared terrorism information;
- Accuracy of identity credentialing and access control to shared terrorism information;
- ISE-SAR EE participants' systems provide a common minimum level of trust for exchanging information among their respective networks and systems;
- ISE-SAR EE participants' systems will get access only to ISE-SAR data that is made available by participating data owners;
- Access to the ISE-SAR EE will be through a single sign-on process based on local credentialing;
- Identity credentials are transmitted and verified in a way that is robust and secure; and
- Participants in the ISE-SAR EE will use an approved identity management process.

5.2.2.2 Objective Outcomes

Specific objective outcomes for the access service in the ISE-SAR EE include

- Develop common access and identity management services across all ISE-SAR EE participants as specified in the ISE IdAM Framework[35] which addresses the following:
  - Developing identity adjudication policies;
  - Developing system access policies;
  - Developing attribute based authorization policies;
  - Developing a federated system for access across the ISE-SAR EE; and

[35] Reference *ISE-G-108: ISE Identity and Access Management (IdAM) Framework* and the *ISE EAF, Version 2.0*, available from PM-ISE or at www.ise.gov.

- ◦ At a minimum, the applicable core networks' authorization and authentication services are used for ISE-SAR EE access.
- Participant data owners providing data that requires special protection caveats will tag their data accordingly, and a future developed attribute-based access service will allow only users with the proper authorization attributes to gain access; this attribute-based access authorization service is a future ISE requirement and is not planned for deployment in the ISE-SAR EE at this time.

The long-term *objective* outcome of this focus area is to grant access to ISE Shared Spaces and ISE-SAR data to *all identified ISE participants* while ensuring the confidentiality, integrity, and availability of the subject data and associated systems.

5.2.3 Affected ISE Core Service Processes

A number of ISE Core service processes support and assist users and their systems in achieving access to data. These are

- **Discovery** – Discovery provides a way for the user to perform federated searches for enterprise content across federated search-enabled data sources via the demonstrated ISE Portal concept. The IdAM component of Discovery provides the service that enables users to access the shared terrorism information in the ISE-SAR EE.
- **Security** – Security services provide confidentiality, integrity, and availability for ISE-SAR EE users. This service would provide the necessary protections for controlling accesses and transmission from ISE Shared Spaces and the stored information. An associated ISE Shared Space configuration must ensure information protection consistent with National Institute of Standards and Technology (NIST), DoD, and National Fusion Center guidelines. Appropriate access control is the basis for these security levels
- **Mediation** – Data and services must be stored in a location and manner accessible to and compatible with the search tool. Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchange between data producers and consumers. Mediation services include data transformation and adaptation. In the case of ISE-SARs, this service would accommodate the interfacing of disparate ISE-SAR systems between different ISE-SAR EE participants. Access mediation services are required in order to adjudicate the various Identity and Access Management protocols used by all ISE-SAR EE participants.
- **Enterprise Service Management (ESM)** – ESM is the continuous process of managing, measuring, reporting, and improving the QoS of ISE-SAR systems and applications. ESM monitoring and status alerts will provide users with notifications of failures to access any ISE Shared Spaces. Access is the foundation of this section and monitoring of that access to ensure agreed-upon reliability is required.
- **Storage** – Storage services would include capabilities to achieve content search and delivery via ISE Shared Spaces. This service process applies to the storage of information according to the data formats outlined in the *ISE-SAR Functional Standard*.
- **Collaboration** – Collaboration enables communication and file-sharing amongst ISE-SAR EE participants. Collaboration uses a full range of accessible, hosted, managed, and content storage services, involving various levels of interaction. Collaboration enables ISE SAR-EE users to identify and interface with other ISE-SAR EE participants. Access control

for collaborated services will allow for a single sign-on protocol that can adjudicate identities across the ISE-SAR EE. Credential adjudication mechanisms are required in order to negotiate the various identity credentials presented by ISE-SAR EE participants for access to services. In turn, Service Providers present these same credentials to the adjudication mechanism for identity assurance validation. These mechanisms will be based on a brokered trust model that embraces all the ISE-SAR EE participants.

5.2.4 Constraints

While there is a need to provide ISE-SAR data broadly across the ISE-SAR EE, there are constraints on information sharing, based on not only the type of information collected and the purposes for which it was collected, but also the functions being performed by the requester of the information.

- The information in the ISE-SAR EE will be used for official criminal law enforcement and homeland security purposes only, and the information could be accessed or used for any other purpose, including general licensing, employment, eligibility for Federal or State benefits, or background investigations, but any use of the information for these purposes must be verified;
- Access will be limited to ISE-SAR EE participant personnel and they will have access to ISE Shared Spaces for testing purposes; and
- For the ISE-SAR EE the use of two factor authentication is not required; however, username and password as well as two factor authentications are allowed. The ISE IdAM Framework technical standard will not dictate what authentication technology or strength will be used, but will allow for various levels of Authentication and Access to shared terrorism information.

5.3 Information Assurance (IA)

Based on the requirements set forth in the *National Strategy for Information Sharing*, in order for terrorism information sharing to take place, mutually acceptable, or common, information security and assurance standards will be used throughout the ISE-SAR EE.

IA is defined as the protection of information and information system(s) from unauthorized or inadvertent access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability to terrorism information shared across the ISE community.

5.3.1 Description[36]

IA covers all aspects of an information system(s) (people, processes, and technology) and all actions necessary to protect, detect, and respond to threats. The use of appropriate management, operational, and technical safeguards mitigates adverse impacts to the organization, individuals, outside entities, or the Nation resulting from use of the information system(s). This includes, specifically for this ISE-SAR EE, terrorism information in transit and at rest must be protected from corruption, from non-disclosure, and from denial of service. This also includes appropriate safeguards pertaining to protection and use of CUI information consistent with CUI policies and guidelines based on the President's *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information (CUI)*.

5.3.2 Outcomes

The general *threshold* outcomes for the focus area of IA are to ensure, for purposes of the ISE-SAR EE initiative, the confidentially, integrity, and availability of ISE-SAR data and ISE Shared Spaces.

5.3.2.1 Threshold Outcomes

From a threshold outcome perspective, the IA service in this ISE-SAR EE must ensure

- Protection of shared terrorism information while being accessed for viewing;
- Protection of shared terrorism information at rest (stored);
- Protection of shared terrorism information from corruption;
- Protection of shared terrorism information from unauthorized disclosure; and
- Protection of shared terrorism information from denial of service.

Note: these IA protections are provided by the core networks that host their applicable ISE Shared Spaces.

5.3.2.2 Objective Outcomes

- The long-term *objective* outcome of the focus area of IA is to provide confidentiality, integrity, and availability of ISE-SAR data and related systems for *all identified ISE participants*.

[36] Source Documentation: *National Strategy for Information Sharing* (October 2007); *National Institute of Standards (NIST) Special Publication 800-39* (Risk Management Framework); *NIST Special Publication 800-53* (Recommended Security Controls for Federal Information System); *NIST Federal Information Processing Standard FIPS-199* (Standards for Security Categorization of Federal Information and Information Systems; BJA Suspicious Activity Reporting (SAR) proposal (May 28, 2008); *ISE-G-106: Technical Standard (Information Assurance), Version 1.0*; *ISE PAIS, Version 1.0*; *ISE EAF, Version 2.0*; Draft Fusion Center Baseline Capabilities.

5.3.3 Affected ISE Core Service Processes

A number of related ISE Core service processes support and assist users and their systems in achieving access to terrorism information. IA provides the confidentiality, integrity, and availability for this access. These ISE Core Services include

- **Discovery** – Discovery also provides a way for the ISE-SAR EE user to perform federated searches for content across federated search-enabled data sources via the demonstrated ISE Portal concept.
- **Security** – Security services provide confidentiality, integrity, and availability for ISE-SAR EE participants. This service would provide the necessary protections for controlling accesses and transmission from/to ISE Shared Spaces and the stored information. The supporting systems must ensure information protection consistent with NIST, DoD, and National Fusion Center guidelines.
- **Mediation** – Data and services must be stored in a location and manner accessible to and compatible with the search tool. Data and services in an enterprise environment are represented in a variety of formats. Mediation services help bridge information exchange between data producers and consumers. Mediation services include data transformation and adaptation. In the case of ISE-SARs, this service would accommodate the interfacing of disparate ISE-SAR systems between different ISE-SAR EE participants.
- **Enterprise Service Management (ESM)** – ESM is the continuous process of managing, measuring, reporting, and improving the QoS of ISE-SAR EE systems and applications. ESM monitoring and status alerts will provide users with notifications of failures to access any ISE Shared Spaces.
- **Storage** – Storage services would include capabilities to achieve content search and delivery via ISE Shared Spaces. This process would be applicable to the storage of information according to the data formats outlined in the *ISE-SAR Functional Standard*.
- **Collaboration** – Collaboration enables communication and file-sharing among users via the ISE-SAR EE. Collaboration uses a full range of accessible, hosted, managed, and content storage services, involving various levels of interaction. Collaboration enables ISE-SAR EE users to discover others based on availability.

5.3.4 Constraints

While there is a need to provide ISE-SAR data broadly across the ISE-SAR EE, there are existing constraints on information sharing based not only on the type of information collected and the purposes for which it was collected, but also the functions being performed by the requester of the information.

- The information in the ISE-SAR EE will be used for official criminal law enforcement and homeland security purposes only, and the information could be accessed or used for any other purpose, including general licensing, employment eligibility for Federal or State benefits, or background investigations, but any use of the information for these purposes must be verified; and
- Access will be limited to ISE-SAR EE project personnel, selected law enforcement agency personnel, and selected Federal participants (FBI, DHS, DoD, and the NCTC).

5.4 Resource/Network Management

The purpose of this section is to identify the appropriate functionality and outcomes required to support, operate, and manage the shared resources across the ISE-SAR EE as guided by CTISS. This includes the provisioning of the capabilities and business/outcomes as described in the previous sections of this document such as Access, Federated Search (associated with the ISE-SAR process of view-only Data Retrieval/Distribution), and Information Assurance.

5.4.1 Description[37]

This functionality would provide the necessary components to manage the elements of a secure, flexible, robust, high performance, and dynamic ISE-SAR EE distributed systems infrastructure allowing users on multiple networks to interface with up to 12 of the ISE-SAR EE sites. The ISE-SAR EE resource and network management services will be built upon existing technologies being used, as appropriate, by the current ISE-SAR EE participating organizations. The functionality for Web integration supports the management of shared resources and infrastructure across a complex ISE-SAR EE.

There is value in integrating currently available systems access to support the ISE-SAR EE. However, the potential use of multiple networks would provide strong reliance on each network to meet the needs of the ISE-SAR EE while retaining the importance of each network community's ownership to meet the needs of its current stakeholders. Considerations must be evaluated to weigh the abilities of current CUI network providers, as appropriate, including the assets and potential cost savings they bring to the table, with the requirements of the full ISE-SAR EE participant community in meeting security, integrity, and performance levels.

The following is a decomposition of the demonstrated functionality required to manage the Web integration and infrastructure resources for this ISE-SAR EE:

- *Network Manager and Systems Manager* – Coordinate network services that will monitor and manage, to include configuration management, network activity, and resources such as network traffic, auditing, servers, and connectivity across the ISE-SAR EE. This will include supporting the capability of a "no failover" infrastructure network whereby the Manager will redirect, if available, network traffic and activities when a server failure occurs or drops connectivity. If correctly and properly configured, the Manager will be enabled to bring failed servers or connections back online. The Manager will monitor and coordinate the network flow of activity whereby the appropriate network scalability can be addressed based on ISE-SAR EE site network activity.
- *Web Services Manager (WSM)* – Coordinate the management and the orchestration of Web services for efficient execution within the ISE-SAR EE. The WSM service will facilitate the loose coupling of executable Web or infrastructure services whereby their location and functionality can be transparent to the network with the exception of the WSM. The WSM will also manage the services and resources of a multi-threaded query such as a federated search. For this ISE-SAR EE, WSM offers the following core competencies from the *ISE EAF* as listed in Table 5-2.

[37] Source Documentation: *NSI CONOPS*; *ISE-SAR Functional Standard, Version 1.0*; *ISE EAF, Version 2.0*; CTISS Technical Standards.

Table 5-2. WSM Core Competencies

Core Competencies	Description
Monitoring and ensuring QoS of critical components	Generates a report about service health and notifies service providers about any unusual signs.
Monitoring Service Level Agreements (SLAs) compliance	Assists service providers in achieving service promises by monitoring service-level objectives and alerting service providers when service-level objective indicator value gets close to threshold.
Providing detection and handling of exceptions	Enables defining exception conditions, detecting and alerting exceptions, and automatically taking corrective actions to handle exceptions in real-time.
Providing insight into the usage of services	Captures usage data such as service throughput and service consumer information, helping with the evaluation of whether a service is useful, worthwhile to continue supporting, and if more services or forwarded staging are needed.
Providing distributed management of services	Offers IT asset managers and service providers the ability to configure, manage, and track distributed services remotely.
Accepting and responding to customer feedback	Will provide a means to receive customer feedback, input, monitor, and resolve issues.

- *ISE Portal* – Provide demonstrated portal access through a single point of entry into the ISE-SAR EE via the local network log-on. This is a more efficient and controlled method of access to the ISE-SAR EE that includes the capability to log and track user activity within the demonstrated ISE Portal once authentication has occurred.
- *Network Appliances* – Network services that are integrated to maintain a persistent and high availability access and data transport in the ISE-SAR EE. These services will manage the network traffic and flow of information in a complex and dynamic environment regardless of network scalability requirements.

5.4.2 Outcomes

In general the outcomes for Resource/Network Management are to enhance the existing ISE-SAR EE infrastructure layout with the appropriate capabilities to manage resources/network infrastructure driven by the new capabilities as defined in other sections of this document. This enhancement includes the construction of a more efficient, robust, resourceful, and higher performing network operating environment.

5.4.2.1 Threshold Outcomes

The ISE-SAR EE infrastructure will operate at the appropriate level and beyond to meet the benchmark network performance requirements as established by the CTISS Technical Standards, including but not limited to 24/7 network availability, network stability and reliability, and replicated infrastructure resources such as database servers and network devices.

5.4.2.2 Objective Outcomes

The ISE-SAR EE infrastructure will enable scalability and support an expanded resource and network capability that can be leveraged by other ISE mission areas.

5.4.3 Affected ISE Core Service Processes

The following ISE Core Service processes defined in this Segment Architecture are affected by the ISE-SAR EE. They are

- *Discovery* – The Web services that will enable this capability are managed and orchestrated by the Web Service Manager. This technology will support multiple instances of a search on ISE-SAR data in the ISE-SAR EE.
- *Security* – The information captured in the log files and registries of the Network Manager, Systems Manager, and the ISE Portal will provide the information assurance, to include monitoring system security, and process network activity data as part of its validation procedures.

5.4.4 Constraints

The ISE-SAR EE will be built upon existing participant systems capabilities, as appropriate, under the guidance of the CTISS Technical Standards. Since the ISE-SAR EE is constructed of multiple technical "Domains," it is considered to be a federated "network" infrastructure with no centralized process for any of the technologies described above.

5.5 Trending/Analysis

5.5.1 Description[38]

Tending and analysis of performance measures data will allow the PM-ISE to determine if the business outcomes of the ISE-SAR EE have been achieved. The process begins with a thorough understanding of the AS-IS state of ISE-SAR processes at participating organizations. The AS-IS assessment will establish the baseline for the performance measures described in Section 3. The project team will identify the key stakeholders for each measure, and work with them to select appropriate data sources, gather data, and conduct analysis. All analysis will be vetted with stakeholders before any findings are presented to senior leaders.

General progress, input, throughput, output, and outcome measures data will be collected regularly over the course of the project. This data will be compared with the AS-IS state to determine if ISE-SAR processes are maturing.

5.5.2 Outcomes

Trending and analysis will enable the PM-ISE to determine whether the desired ISE-SAR EE business outcomes and performance goals have been achieved. By collecting data periodically, the project team will also be able to assess the degree to which ISE-SAR processes have been improved at a given site.

[38] Source Documentation: Performance Measurement for Justice Information System Projects, (Bureau of Justice Assistance, United States Department of Justice, March 2008).

5.5.3 Affected Processes

The proposed outcomes and performance measures are designed to assess the complete ISE-SAR information flow. Therefore, trending and analysis affects all processes.

5.5.4 Constraints

Data availability will be the primary trending and analysis constraint. In particular, gathering performance outcome data will be difficult without the cooperation of law enforcement organizations such as the FBI and JTTFs. In order to overcome this constraint, the project team will seek agreements with data owners at these organizations in the early stages of the project.

6 Summary

This ISE-SAR EE Segment Architecture document has outlined the business and functional drivers, information exchange requirements, outcomes and constraints for the ISE-SAR EE project. This document has also identified those EE enabling services required for operational implementation and use throughout the ISE-SAR EE. These services are effected through procedural, operational, and technical implementation efforts at and between ISE-SAR EE sites, and will drive necessary decisions (both programmatic and solution) consistent with the business case for the ISE-SAR EE. With the identification of ISE CORE Services to be demonstrated across the ISE-SAR EE, this Segment Architecture lays the foundation for building executable, long-term operational IT solutions for the ISE.

The *ISE-SAR EE Solution Architecture*, developed subsequent to and consistent with this Segment Architecture, will incorporate attributes from this Segment Architecture and leverage existing capabilities when appropriate. The Solution Architecture will also document which business and functional capabilities will be Threshold or Objective for implementation, primarily based upon resource availability. As part of this ISE-SAR EE, partnering ISE-SAR EE organizations will follow guidance from both this Segment Architecture and the corresponding *ISE-SAR EE Solution Architecture* to define ISE-SAR EE project development, implementation, and operations activities.

This page intentionally blank.

Appendix A: Summary of Threshold and Objective Outcomes

For ISE-SAR EE participants and ISE Implementation Agents of ISE Core services and capabilities, the following are summaries of specific drivers for the *ISE-SAR EE Solution Architecture* and detailed implementation guidance based on Threshold and Objective descriptions extracted from this Segment Architecture. This Appendix provides a quick reference of those outcomes.

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
SAR PROCESS: ORGANIZATIONAL PROCESSING	Each ISE-SAR EE participant system will make all ISE-SARs accessible to all other ISE-SAR EE participants in the Summary ISE-SAR Information format (i.e., with no privacy fields).	Each ISE-SAR EE participant system will share ISE-SARs to the applicable State and major urban area Fusion Center in the Detailed ISE-SAR IEPD format of the *ISE-SAR Functional Standard* and with all other ISE-SAR EE participants to the maximum extent permitted by its laws, regulations, and policies. This is contingent on meeting privacy requirements documented in Section 5.1.	4.5.2
SAR PROCESS: ORGANIZATIONAL PROCESSING	Each ISE-SAR EE participant system processes SARs consistent with the *ISE-SAR Functional Standard*, ISE Privacy Guidelines, and supplementary implementation guides.		4.5.2
SAR PROCESS: ORGANIZATIONAL PROCESSING	Each ISE-SAR EE participant system will be capable of accessing free-text, depersonalized (no personal information) ISE-SARs (ISE-SAR “Summary Reports”) contained in the SAR Summary Reports Library.		4.5.2
SAR PROCESS: INTEGRATION/ CONSOLIDATION	Each ISE-SAR EE participant system processes and stores all ISE-SARs in their ISE Shared Space consistent with the *ISE-SAR Functional Standard*, ISE Privacy Guidelines, and supplementary implementation guides.		4.6.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
SAR PROCESS: INTEGRATION/ CONSOLIDATION	ISE-SAR EE sites may store Detailed ISE-SAR IEPDs in their ISE Shared Spaces if they meet the reasonable suspicion threshold, however they must also demonstrate that the necessary privacy and civil liberties policy framework is in place, both at their site and the viewing site(s), in order to share Detailed ISE-SAR IEPD records. If the necessary policy framework is not in place at the ISE-SAR EE site and the viewing site(s), only Summary ISE-SAR Information formatted records (exclusive of personal information) may be shared from the respective ISE Shared Space.		4.6.2
SAR PROCESS: INTEGRATION/ CONSOLIDATION	Each ISE-SAR EE participant manages and maintains the ISE-SARs submitted to its ISE Shared Space. The owner of the ISE Shared Space may not in all cases be the source originator of the SAR data. In addition, the same incident or suspicious behavior may be reported by more than one organization.		4.6.2
SAR PROCESS: INTEGRATION/ CONSOLIDATION	ISE-SAR data in ISE Shared Spaces is available for search and viewing to all the approved users of the ISE-SAR EE.		4.6.2
SAR PROCESS: INTEGRATION/ CONSOLIDATION	Only the ISE-SAR EE participant managing an ISE Shared Space, or the originator of the ISE-SAR, may update/modify/delete the ISE-SARs hosted in that ISE Shared Space.		4.6.2
SAR PROCESS: DATA RETRIEVAL/ DISTRIBUTION	Search Participating ISE Shared Spaces in the ISE-SAR EE: • Authentication for access and search will be controlled consistent with guidance from the ISE IdAM Framework and the Technical Standard: Information Assurance.	Search Participating ISE Shared Spaces – ISE-SAR data in participating ISE Shared Spaces should be accessible and searchable through an integrated, federated process. The search capability should be able to identify needed information through flexible queries. This tool should allow a user to find known data as well as to discover information previously unknown to the requestor. • *Search/Query Participating ISE Shared Spaces*: The search capability must be able to query participating ISE Shared Spaces.	4.7.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
		ISE Shared Spaces will be configured to use an internal search process. The federated search function must accommodate internal search capability to query the database and receive the resulting information; • *Selectively Query ISE Shared Spaces:* The tool should be capable of searching or querying one or more selected ISE Shared Spaces as well as performing broad area searches of all relevant ISE Shared Space; • *Search Unstructured/Semi-Structured (Non-database) Data in the SAR Summary Reports Library:* Some data are in non-database formats (e.g., documents, reports, various free text formats). There must be a search capability to conduct word searches in such formats; • *Maintain Maximum Availability:* The search tool should be useable across a broad spectrum of users participating in the ISE-SAR EE; • *Integrate Results (Federated Search):* The search tools should be capable of providing a consolidated presentation of the search results, be they from a single ISE Shared Space or the results of queries from multiple ISE Shared Spaces; and • *Enable Data Screening or Preview:* The initial results list shall display submitting organization, contact information, and information sought. The search capability should be able to sort the initial search results based on the categories of information displayed.	

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
SAR PROCESS: DATA RETRIEVAL/ DISTRIBUTION	Identify and View Relevant Information from the SAR Summary Reports Library and ISE Shared Spaces • The search capability displays results from “Summary Reports” within the SAR Summary Reports Library, based on unstructured text searches; • The search capability displays results drawn from ISE Shared Spaces participating in the ISE-SAR EE; • The information is displayed accurately and completely reflects the data in the ISE Shared Spaces.		4.7.2
SAR PROCESS: DATA RETRIEVAL/ DISTRIBUTION	In conducting the search function across ISE Shared Spaces, inadvertent or unauthorized release of sensitive and/or personal information must be prevented. • *Protect Personal Information from Unauthorized Access:* Personal information within the ISE Shared Spaces shall be protected, consistent with public law and policy governing protection of personal information. • *Provide Audit Tracking:* The search capability shall log information about the organization of the originator of the search, including the originator’s authorization or permissions, the justification for the search, the time and date of the search, and an optional reference number field will also be provided.		4.7.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
SAR PROCESS: DATA RETRIEVAL/ DISTRIBUTION		Display needed data from participating ISE Shared Spaces—Once found, the information should be viewable from participants' ISE Shared Spaces by any authorized requestor. • *View Information:* An authorized user should be able to view all ISE-SAR data responsive to the query that exists in participating ISE Shared Spaces subject to established limits on the number of records that can be accessed in response to an inquiry; • *Accurately Display Information:* The search results must accurately reflect the data extant in the ISE Shared Spaces, displayed without unintended alteration or introduced errors on the user's desktop computer; and • *Failed Contact Indicator:* The search capability should indicate any failures to access ISE Shared Spaces.	4.7.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
SAR PROCESS: FEEDBACK	ISE-SAR EE participant systems continually measure and verify that the *ISE-SAR Functional Standard* effectively meets the needs of law enforcement agencies. • Examine the capabilities of the automated ISE-SAR collection and reporting systems currently used by ISE-SAR EE participants to identify areas of commonality and gaps when compared to the *ISE-SAR Functional Standard* elements; • Evaluate whether ISE-SARs contributed to the SAR Summary Reports Library or made available to a participant's ISE Shared Space conform to the ISE-SAR criteria specified in the *ISE-SAR Functional Standard*. • Measure the effectiveness of search tools in retrieving ISE-SAR data based upon unstructured search parameters in either ISE Shared Spaces or the SAR Summary Reports Library. • Measure the usage of the ISE-SAR EE over the evaluation period. • Provide mechanism(s) to alert participants when an ISE-SAR is found to have been designated in error.	ISE-SAR EE participants' measure and verify that the *ISE-SAR Functional Standard* (ISE-SAR designation criteria and information formats) meets the needs of law enforcement agencies and that user feedback informs required version updates to the *ISE-SAR Functional Standard* to reflect the needs of the law enforcement community and the ISE. The following high-level sub-objectives are planned: • Based on the ISE-SAR EE, verify the *ISE-SAR Functional Standard* criteria for completeness and usefulness in a multi-agency Federal, and SLT user base; • Follow the governance framework described in ISE-SAR EE and ISE documentation to ensure that common definitions of suspicious behavior identified by participating agencies are codified and implemented to the greatest extent possible. • Based on the ISE Shared Spaces model, examine the *ISE-SAR Functional Standard* to ensure that the ISE-SAR data model in the IEPD component fully captures desired information sharing components and is consistent with on-going LEXS and/or NIEM/UCORE initiatives.	4.8.2
SAR PROCESS: FEEDBACK		Establish appropriate capabilities in systems to improve collaboration between investigators and analysts in multiple agencies to • Improve situational awareness within the law enforcement community and private sector; • Link disparate investigations or incidents to common SAR activity; • Solve or interdict criminal activities with potential terrorist connections.	4.8.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
SAR PROCESS: FEEDBACK		Establish the systems' capabilities for law enforcement agency investigators and analysts to identify best practices, lessons learned, or success stories with ISE-SAR EE systems that the participants and other members of the ISE-SAR EE may choose to adopt.	4.8.2
SAR PROCESS: FEEDBACK		Establish appropriate capabilities in ISE-SAR EE systems for improving collaboration between investigators and analysts in multiple agencies to • Provide mechanisms to deliver feedback to originating agencies, when/if a submitted SAR becomes an ISE-SAR. • Measure the comparative frequency of ISE-SAR EE participants' submissions to the SAR Summary Reports Library and to ISE Shared Spaces. • Establish survey tools, user groups, or on-line interview process capabilities to solicit end-user feedback on whether the ISE-SAR EE systems helped analysts create new cases, link previous disparate cases or incidents, or helped solve or interdict potential terrorism-based crimes or activities.	4.8.2
SAR PROCESS: FEEDBACK		Establish the systems' capabilities for law enforcement agency investigators and analysts to identify best practices, lessons learned, or success stories and share that information within the law enforcement community. • Establish an on-line repository for end-users to contribute best practices, lessons learned, and success stories that may assist investigators and analysts in identifying and interdicting terrorist activities.	4.8.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
PRIVACY	ISE-SAR EE mechanisms (procedural, operational, and technical) will ensure that Detailed ISE-SAR IEPDs (ISE-SARs with personal information) do not violate civil rights and civil liberties, and that they adhere to policies regarding, for example, First Amendment protections or those that prohibit racial, ethnic, or religious profiling.		5.1.2
PRIVACY	ISE-SAR EE sites may store Detailed ISE-SAR IEPDs in their ISE Shared Spaces if the site possesses the appropriate privacy and civil liberties policy framework and the SARs meet the requirement of the *ISE-SAR Functional Standard* to have a potential nexus with terrorism-related criminal activity. In addition, in order to share Detailed ISE-SAR IEPD records, the EE sites also must demonstrate that the viewing site has implemented the necessary privacy and civil liberties policy framework. Absent the necessary policy framework at the ISE-SAR EE site and the viewing site(s), only Summary ISE-SAR Information formatted records (exclusive of personal information) may be shared from the submitting agency's ISE Shared Space.		5.1.2
PRIVACY		Non-Federal ISE-SAR EE participants will develop and implement privacy policies that afford privacy and civil liberties protections at least as comprehensive as those developed for Federal entities under the ISE Privacy Guidelines.	5.1.2
PRIVACY		Federal ISE-SAR EE participants that disseminate or retrieve ISE SARs using the Detailed ISE-SAR IEPD will ensure that data in ISE-SAR systems/ISE Shared Spaces is protected consistent with an ISE-Privacy Guidelines-compliant privacy policy.	5.1.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
ACCESS		Develop common access and identity management services across all ISE-SAR EE participants as specified in the ISE IdAM Framework which addresses the following: • Developing identity adjudication policies • Developing system access policies • Developing attribute based authorization policies • Developing a federated system for access across the ISE SAR EE • At a minimum, the applicable core networks' authorization and authentication services are used for the ISE-SAR EE access.	5.2.2
ACCESS		Participant data owners providing data that requires special protection caveats will tag their data accordingly and a future developed attribute-based access service will allow only users with the proper authorization attributes to gain access; this attribute-based access authorization service is a future ISE requirement and is not planned for deployment in the ISE-SAR EE at this time.	5.2.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
ACCESS	Access service in the ISE-SAR EE must ensure • Security of identity credentialing and access control to shared terrorism information • Currency of identity credentialing and access control to shared terrorism information • Accuracy of identity credentialing and access control to shared terrorism information • ISE-SAR EE participants' systems provide a common minimum level of trust for exchanging information among their respective networks and systems • ISE-SAR EE participants' systems will get access only to ISE-SAR data that is made available by participating data owners • Access to the ISE-SAR EE will be through a single sign-on process based on local credentialing • Identity credentials are transmitted and verified in a way that is robust and secure • Participants in the ISE-SAR EE will use an approved identity management process		5.2.2
INFORMATION ASSURANCE		Provide confidentially, integrity, and availability of ISE-SAR data and related systems to *all identified ISE participants*.	5.3.2
INFORMATION ASSURANCE	Protection of shared terrorism information while being accessed for viewing.		5.3.2
INFORMATION ASSURANCE	Protection of shared terrorism information at rest (stored).		5.3.2
INFORMATION ASSURANCE	Protection of shared terrorism information from corruption.		5.3.2
INFORMATION ASSURANCE	Protection of shared terrorism information from unauthorized disclosure.		5.3.2
INFORMATION ASSURANCE	Protection of shared terrorism information from denial of service.		5.3.2

Topic Area	Threshold Description	Objective Description	Segment Architecture Section Reference
RESOURCE/ NETWORK MANAGEMENT	The ISE-SAR EE infrastructure will operate at the appropriate level and beyond to meet the benchmark network performance requirements as established by the CTISS Technical Standards, including but not limited to 24/7 network availability, network stability and reliability, and replicated infrastructure resources such as database servers and network devices.	The ISE-SAR EE infrastructure will enable scalability and support an expanded resource and network capability that can be leveraged by other ISE mission areas.	5.4.2

This page intentionally blank.

Appendix B: Glossary of Terms

Access Control—Limiting access to information system resources only to authorized users, programs, processes, or other systems. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Agency Transport—Infrastructure (including cabling, network components, and protocols) that enables the movement of data between agencies participating in the ISE SAR EE.

Agency—Has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code (i.e., an Executive department, a Government corporation, and an independent establishment), together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office. [EO 13388 Section (6)(a) and 5 U.S.C. 105]

Authentication—Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Authorization—Access privileges granted to a user, program, or process. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Availability—Timely, reliable access to data and information services for authorized users. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Business Analytical Services—Supports "the extraction, aggregation, and presentation of information to facilitate decision analysis." [http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Business Reference Model (BRM)—A framework facilitating a functional (not organizational) "view of the Federal Government's lines of businesses (LoBs), including its internal operations and its services for citizens, independent of the agencies, bureaus, and offices that perform them." [http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Common Services—In a service-oriented architecture, Web services are divided into two broad categories: Line of Business Services and Common Services. Common Services are those services employed by a large subset of users. These services are provided centrally by an enterprise authority to assure interoperability and maximize reuse.

Community of Interest (COI)—COI is defined in the National Information Exchange Model (NIEM) Concept of Operations (CONOPS), October 2004, as a collaborative group of users who require a shared vocabulary to exchange information in pursuit of common goals, interests, and business objectives.

Confidentiality—Assurance that information is not disclosed to unauthorized individuals, processes, or devices. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Controlled Unclassified Information (CUI)—Categories of unclassified information that require controls that protect the information from public release, both to safeguard the information privacy and other legal rights of U.S. citizens and to deny information advantage to those who threaten the security of the Nation.

Core Enterprise Services (CES)—Services that enable both service and data providers on the "net," by providing and managing the underlying capabilities to deliver content and value to end-users.

Criminal Intelligence Coordinating Council (CICC)—Criminal Intelligence Coordinating Council (CICC) under the Global Justice Information Sharing Initiative (Global) sets national-level policies to implement the *National Criminal Intelligence Sharing Plan* and monitor its progress at the state and local level. The CICC works with the Department of Justice's Law Enforcement Information Strategy Initiative and with the Justice Intelligence Coordinating Council, created by a directive of the Attorney General, to improve the flow of intelligence information among Federal, State, and local law enforcement agencies.

Cross-Agency Initiative—An effort supported with resources (including staff, products, information, and/or funding) from multiple Federal agencies for the mutual benefit of all.

Cross-Domain Security—An integrated, comprehensive, and consistent approach to addressing the shared risk associated with the connection of networks of different classification levels.

Data Accessibility—Those functional capabilities of the ISE-SAR EE that allow a user of the ISE SAR EE to obtain data when needed. In particular, data accessibility depends on the principles that all data shall be posted to ISE Shared Spaces and tagged with metadata to enable access to all users except when limited by security, policy, or regulations.

Data Context—Any information that provides additional meaning to data. Data Context typically specifies a designation or description of the application environment or discipline in which data is applied or from which it originates. It provides perspective, significance, and connotation to data and is vital to the discovery, use, and comprehension of data. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Description—A rich description of data, thereby supporting its discovery and sharing. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Interoperability—The capability of different programs to exchange data via a common set of business procedures and to read and write the same file formats and use the same protocols.

Data-in-Transit—Data is typically referred to as being in one of three states at any time: (1) at rest, (2) processing, or (3) in transit. Data-in-Transit refers to the state in which data is being passed from one physical location to another via the ISE Core Transport. Data is in transit when it is passing over physical cables, being transmitted over wireless networks and satellite links, and passing through routers and other network components.

Data Reference Model (DRM)—One of the five reference models of the Federal Enterprise Architecture (FEA). The DRM is a framework whose primary purpose is to enable information sharing and reuse across the Federal Government via the standard description and discovery of common data and the promotion of uniform data management practices. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Sharing—Describes the sharing and exchange of data, where sharing may consist of ad-hoc requests (such as a one-time query of a particular data asset), scheduled queries, and/or exchanges characterized by fixed, re-occurring transactions between parties. It involves exchanges within and between agencies and COIs to support mission-critical capabilities. Finally, it eliminates duplication and/or replication of data, thereby increasing data quality and integrity. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Trustability—Those functional capabilities of the ISE-SAR EE that enable a user to place a value on specific data provided in the ISE-SAR EE. In particular, Data Trustability depends on the principle that data shall be tagged with metadata describing its pedigree, source, timeliness, confidence, or other attributes associated with trust.

Data Understandability—The functional capabilities of the ISE-SAR EE that enable a user to properly interpret specific data and use that data in an appropriate manner. In particular, Data Understandability depends on the principle that data shall be tagged with metadata describing its pedigree, source, timeliness, and perhaps description. Even more important, however, is that data be described in standard ways using common terminology as established by negotiated and accepted taxonomies.

Data Visibility—The functional capabilities of the ISE-SAR EE that reveal the existence of specific data to a user of the ISE-SAR EE. In particular, data visibility depends on the principles that all data shall be posted to ISE Shared Spaces and tagged with metadata to enable discovery of data by users.

Detailed ISE-SAR IEPD—Technical artifacts (data model, data schema, and reference vocabulary) in the *ISE SAR Functional Standard* providing descriptions and relationships of all ISE-SAR data that may be exchanged, including data tagged elements (using metadata markup technology) requiring protection under privacy laws and regulations (designated as privacy fields or privacy information). In the Detailed ISE-SAR IEPD, all 189 data fields can be made available by the data owner to external ISE-SAR EE participants consistent with privacy policies and meeting the criteria threshold as defined in the *ISE-SAR Functional Standard* regarding information collected with the potential nexus with terrorism-related crime.

Digital Signature—Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Synonymous with electronic signature. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Domain—A virtual environment governed by a single set of consistent policies. These policies include, but need not be limited to, security policies that govern authentication, authorization, availability, confidentiality, and integrity. Typically a domain is managed by a single organizational entity, such as a single agency, that enforces the applicable policies, e.g., the Central Intelligence Agency (CIA) domain. A group of agencies may also establish a new domain for sharing information by agreeing on a consistent set of policies for the data stored in that domain and designating a proxy to manage that domain, e.g., the Intelligence Domain.

Enabling Technology—Any technological capability used to support ISE-SAR EE policies or business processes.

Encryption—The process of obscuring information to make it unreadable without special knowledge.

Enterprise Architecture (EA)—A strategic information asset base that defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs.

Enterprise Search—The act of searching content to discover data, information, and knowledge wherever it exists.

Extensible Markup Language (XML)—XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML). Originally designed to meet the challenges of large-scale electronic publishing, XML also plays an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. [http://www.w3.org/XML/]

Federal Enterprise Architecture—A business-driven framework that defines and aligns Federal business functions and supporting technology and includes a set of five common models (performance, business, service component, data, and technical).

Fusion Center—A center established by State and major urban area governments designed to coordinate the gathering, analysis, and dissemination of terrorist-related, law enforcement, and public-safety information.

Global Justice Information Sharing Initiative (Global)—Serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

Homeland Security Information—Any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))]

Identity and Access Management (IdAM)—An overarching term often used to refer to the processes of authentication, authorization, assignment of attributes and privileges, access management, credential issuance, and the identification of a digital identity and the binding of that digital identity to an individual.

Information Assurance—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Information Sharing Council (ISC)—The Information Sharing Council was established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection 1016(g) of the IRTPA. [Extracted from IRTPA 1016(a)(1)] EO 13388, which superseded EO 13356, established the Information Sharing Council.

Information Sharing Environment (ISE)—An approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)]

Integrity—Quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Interoperability—The capability of different programs to exchange data via a common set of business procedures and to read and write the same file formats and use the same protocols.

Intrusion Detection—The act of detecting actions that attempt to compromise the confidentiality, integrity, or availability of a resource. It does not necessarily prevent intrusion from occurring.

ISE Implementation Agent—An organization responsible for providing infrastructure and services in the ISE Core.

ISE Participant—Any Federal, State, local, or tribal government organization; private sector entity; or foreign government organization that participates in the ISE.

ISE-SAR—A SAR that has been determined to have a potential terrorism nexus.

ISE-SAR EE Participant—Any Federal, State, local, or tribal government organization, or private sector entity that is participating in the ISE-SAR EE project.

ISE Shared Spaces—The ISE Shared Spaces concept is a key implementation approach for developing trust and community-wide information sharing across the entire ISE. ISE Shared Spaces are networked data and information repositories used to make standardized terrorism-related information, applications, and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities). While ISE Shared Spaces are accessible in each of the three ISE security domains (CUI/SBU, Secret, and TS/Sensitive Compartmented Information), for this ISE-SAR EE, ISE Shared Spaces will be implemented for the CUI/SBU domain only.

ISE Transport—That infrastructure (including cabling, network components, and protocols) that enables the movement of data between agencies participating in the ISE (synonymous with Agency Transport).

Justice Reference Architecture (JRA)—The blueprint that enables interoperability, guides implementation, and facilitates understanding among disparate communities in the law enforcement communities.

Law Enforcement Information—For the purposes of the ISE-SAR EE only, any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Line of Business—Internal operations of the Federal Government and its services, independent of the agencies that perform them. [http://www.whitehouse.gov/OMB/egov/documents/DRM_2_0_Final.pdf]

Local Government—Refers to (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity. [Homeland Security Act of 2002, 6 U.S.C. 101]

National Security System (NSS)—40 U.S.C. Section 11103(a) defines a national security system as “a telecommunications or information system operated by the Federal government, the function, operation, or use of which: (A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons system; or (E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions. (2) Limitation. – Paragraph (1) (E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).”

Non-repudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Outcome Measures—Outcomes describe the intended result of carrying out a program or activity. They define an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries and/or the public. [OMB Circular A-11]

Person of Interest (POI)—A person or entity about which ISE-SAR EE participants wish to obtain or share information (this term is used interchangeably with Target of Interest in this context).

Personal Information—Information that may be used to identify an individual (i.e., data elements in the identified "privacy fields" of the *ISE-SAR Functional Standard*)

Private Sector Partners—Includes vendors, owners, and operators of products and infrastructures participating in the ISE-SAR EE.

Program Manager (PM)—The person designated under subsection 1016(f) of the IRTPA, who is responsible for information sharing across the Federal Government and shall, in consultation with the Information Sharing Council, plan for and oversee the implementation of, and manage, the ISE. [Extracted from IRTPA 1016(a)(3) and 1016(f)]

Quality of Service (QoS)—The probability of the telecommunication network meeting a given traffic contract, or in many cases a term used informally to refer to the probability of a packet succeeding in passing between two points in the network within its desired latency period.

Role/Privilege Management—Set of functions that protects networks and systems from unauthorized access by persons, acts, or influences and includes many sub-functions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

Security Domain—The term "Security Domain" refers to three security levels—Special Compartmented Information (SCI), Secret, and CUI/Sensitive but Unclassified (SBU)—across which the ISE must operate.

Service—Services provide a standard means of interoperating between different software applications that run on a variety of platforms and/or frameworks. Services are characterized by their interoperability and extensibility. They can be combined in a loosely coupled way in order to achieve complex operations. Programs providing simple services can interact with each other in order to deliver sophisticated value-added services. [http://www.w3.org/2002/ws/Activity]

Service Adaptation—Solves the problem of converting between the rules used by one service into those required by another while maintaining the integrity of the message being sent through the service-based architecture. [http://www.nces.dod.mil/coreServices/mediation_content.aspx]

Service-based Architecture—A business-driven approach to software architecture that supports integrating the business as a set of linked, repeatable business tasks, or "services." Services are self-contained, reusable software modules with well-defined interfaces and are independent of applications and the computing platforms on which they run. Service-based architecture helps users build composite applications, which are applications that draw upon functionality from multiple sources within and beyond the enterprise to support horizontal business processes.

Service Level Agreement (SLA)—SLA defines mutual understandings and expectations between a service consumer and a service provider. The service-level objectives that both the service consumer and the service provider agree upon usually include a set of indicators such as availability and average response time.

Shared Data—The terrorism data collected and maintained by agencies in the course of executing their mission.

State—Any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. [Homeland Security Act of 2002, 6 U.S.C. 101]

Summary ISE-SAR Information—Summary ISE-SAR Information is based on the technical artifacts from the Detailed ISE-SAR IEPD, but the viewable information has the privacy fields (containing personal information) stripped from any results.

Suspicious Activities Report (SAR)—Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention (*ISE-FS-200: ISE-SAR Functional Standard* found at www.ise.gov).

Target of Interest (TOI)—A person or entity of significance, under watch or investigation, who could pose a threat to the United States or U.S. interests.

Technical Reference Model (TRM)—A component-driven, technical framework used to categorize the standards, specifications, and technologies that support and enable the delivery of service components and capabilities. The TRM provides a foundation to categorize the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components that may be used and leveraged in a Component-Based or Service-Oriented Architecture. It also unifies existing agency TRMs and Electronic Government (EGOV) guidance by providing a foundation to advance the re-use of technology and component services from a Government-wide perspective. [http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Terrorism Information—All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals. [IRTPA 1016(a)(4)]

User Applications—Software applications used by one or more ISE user communities wishing to leverage the capabilities of the ISE-SAR EE. User Applications are in contrast to Enterprise Applications, which are used by a large subset of ISE-SAR EE users and provided centrally, or Management Applications, which are used by a small set of administrators to maintain and operate the ISE-SAR EE.

Virtual Private Network (VPN)—A private communications network usually used within a company, or by several different companies or organizations, to communicate from remote locations over an unsecure public network.

Web Service Description Language (WSDL)—WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate. [http://www.w3.org/TR/wsdl]

XML Schemas/XML Schema Definitions (XSD)—Express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content, and semantics of XML documents. [http://www.w3.org/XML/Schema]

This page intentionally blank.

Appendix C: Abbreviations

ASD	Assistant Secretary of Defense
BJA	Bureau of Justice Assistance
BPA	Business Process Analysis
BPWG	Business Process Working Group
BRM	Business Reference Model
CES	Core Enterprise Services
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CICC	Criminal Intelligence Coordinating Council
COI	Community of Interest
CONOPS	Concept of Operations
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DoD	Department of Defense
DoJ	Department of Justice
DRM	Data Reference Model
DSOP	Directorate of Strategic Operational Planning
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EE	Evaluation Environment
EGOV	Electronic Government
EO	Executive Order
ESM	Enterprise Service Management
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FI	Field Interview
FIG	Field Intelligence Group
FS	Functional Standard

G	Guidance
GSRA	geographic-specific risk assessment
HD&ASA	Homeland Defense and America's Security Affairs
HQ	Headquarters
HSIN	Homeland Security Information Network
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IACP	International Association of Chiefs of Police
IC	Intelligence Community
ICE	Immigration, Customs, and Enforcement
IdAM	Identity and Access Management
IEPD	Information Exchange Package Documentation
INTERPOL	International Criminal Police Organization
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council
ISE	Information Sharing Environment
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordinating Group
JRA	Justice Reference Architecture
JTTF	Joint Terrorism Task Force
LE	Law Enforcement
LEXS	Law Enforcement Information Sharing Program Exchange Specification
LoB	Line of Business
MCCA	Major City Chiefs' Association
MCSA	Major County Sheriffs' Association
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSI	Nationwide Suspicious Activity Reporting Initiative
NSIS	National Strategy for Information Sharing
NSS	National Security System

ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PIN	Priority Information Need
PM	Program Manager
PM-ISE	Program Manager, Information Sharing Environment
POI	Person of Interest
QoS	Quality of Service
RAID	Redundant Arrays of Inexpensive Disks
RISS	Regional Information Sharing Systems
RMS	Records Management System
SAR	Suspicious Activity Report (Reporting)
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information (Security Classification)
SGML	Standard Generalized Markup Language
SLA	Service Level Agreement
SLT	State, Local, and Tribal
TMU	Threat Management Unit
TOI	Target of Interest
TRM	Technical Reference Model
TS	Top Secret
TSC	Terrorist Screening Center
TWL	Terrorist Watchlist
UASI	Urban Area Security Initiative
UCORE	Universal Core
UN	United Nations
USC	U.S. Code
VGTOF	Violent Gang/Terrorism Organization File
VPN	Virtual Private Network
WSDL	Web Service Description Language
WSM	Web Services Manager

XML	Extensible Markup Language
XSD	XML Schema Definitions

Appendix D: ISE Shared Spaces

1 Overview

The ISE Shared Spaces concept is a key implementation approach for developing trust and community-wide information sharing across the entire ISE. ISE Shared Spaces are networked data and information repositories used to make standardized terrorism-related information, and applications and services accessible to all ISE-SAR EE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities)[39].

2 Definitions

2.1 General

ISE Shared Space: An ISE Shared Space is where standardized terrorism information, as defined through the Common Terrorism Information Sharing Standards (CTISS), is made available by one ISE-SAR EE participant to others, as appropriate. Additionally, ISE-SAR EE participants may create or use their ISE Shared Space to make services and data accessible, as appropriate, to other participants.

ISE Core: The ISE Core provides infrastructure and services necessary for the interconnection and use of information made available through various ISE Shared Spaces.

2.2 Technical

ISE Shared Space: An ISE Shared Space consists of hardware and software that serve as the ISE-SAR EE participant's infrastructure for ISE activity, as defined through the Common Terrorism Information Sharing Standards (CTISS). There may be multiple ISE Shared Spaces, each under the management, control, and resourcing responsibility of the ISE-SAR EE participant. This responsibility includes ensuring information security, data integrity, use, retention, and other data stewardship requirements are met.

ISE Core: The demonstrated ISE Core in the ISE-SAR EE has three major components: core services, portal services, and core transport. Demonstrated ISE Core Services provide ISE-level services used in operating the ISE-SAR EE (e.g., Discovery, Mediation, Storage, Collaboration, and Security). ISE Portal Services provide the infrastructure for those services used in interfacing the demonstrated ISE Portal to the Core (including Network Management). ISE Core Transport entails the underlying telecommunications infrastructure (e.g., cables, routers, switches) which moves ISE-SAR data and information from one ISE Shared Space to another.

[39] Reference *ISE EAF, Version 2.0* for descriptions of ISE Shared Spaces and the ISE Architecture Program.

3 Models

3.1 ISE Shared Spaces

In describing ISE Shared Spaces for identifying existing infrastructure to implement an ISE Shared Space or in planning for and establishing an ISE Shared Space, three models are to be considered:

- Establishing an information flow-driven model for an ISE Shared Space,
- Logical view model (or system-independent operational descriptions), and
- Hosting and implementation model.

These models support ISE-SAR EE participants in their development of solution architectures that clearly identify the structure and attributes of the organization's ISE Shared Spaces in sufficient detail.

3.1.1 Information Flow Model

The information flow model for implementing an ISE Shared Space considers the mission or business drivers for organizations to follow in interfacing with the ISE-SAR EE. This model takes into account not only the requirements of ISE-SAR EE participants that produce ISE-SAR information but also the information needs of other participants consuming another participant's information. These essentials are easily identified from the defined information flows from mission business processes that define the ISE-SAR EE. These drivers include:

- *Specific Mission:* These information flows would be based upon defined ISE-SAR EE mission business processes presenting relationships, exchanges, and products for terrorism information sharing.
- *Community:* These information flows would be based upon mission business processes of participating organizations that make up a community of interest (COI). They may be associated with defense, homeland security, intelligence, foreign affairs, or law enforcement representative organizations with business processes that are part of that select community. Outputs of these COI processes may be data and information structured under CTISS for storage in an ISE Shared Space.
- *Entity:* These information flows would be based upon mission business processes of an individual organization (i.e., 'entity').

3.1.2 Logical View Model

The logical model identifies three general implementation schemes:

- *Replication:* Storage of terrorism information from internal resources into an ISE Shared Space and making it accessible to other ISE-SAR EE participants using common services, such as discovery, storage, and collaboration for access and use. A common example of this scheme would be libraries that provide the general public on-line card catalog services for locating books yet also maintain their book records on their own internal systems for inventory and management purposes.

- *Web-Service:* Exposing terrorism information, services, and applications via Web services that interface with other ISE-SAR EE participant Web portals as appropriate. A common example of this is the approach used by on-line shopping vendors to make multiple brand product information and sales services accessible to the general public via the Internet.
- *Hybrid:* Allowing direct access, with appropriate access management safeguards, to selected applications and information within an ISE-SAR EE participant's infrastructure. An example is the collaborative use of a Case Management application used by two or more agencies cooperating in a joint CT investigation. Access would be granted after validating and ensuring appropriate authenticating credentials have been verified. An example of this scheme is police departments' accessing DOJ's Joint Automated Booking System (JABS).

3.1.3 Hosting and Implementation Model

Given the logical information flow and models, various hosting and implementation options are available to establish a participant's ISE Shared Space. These hosting options include:

- *Department Level:* A Department, agency, or other ISE-SAR EE participating organization would establish an ISE Shared Space or multiple ISE Shared Spaces to facilitate terrorism information sharing for the entire organization, to include assigned bureaus and subordinate offices.

The ISE Shared Space(s) would be interconnected with other ISE-SAR EE participants to provide access to standard information. An example of such a department-wide application for providing a comprehensive repository of information is the FBI's Regional Data Exchange (R-DEx) or One-DOJ system. One-DOJ is designed to provide the capability to share full text law enforcement investigative information from Federal, State, and local investigative agencies working in association with the FBI. From an overarching programmatic perspective, in this option an ISE-SAR EE participant would continue to be responsible for the overall budgeting, resourcing, and installation of the ISE Shared Space on behalf of the entire organization and its affiliated offices.

- *Component/Other Level:* An organizational element or subcomponent of the larger department, agency, or ISE-SAR EE participant would be responsible for establishing an ISE Shared Space supporting that component's responsibilities for interfacing with the ISE-SAR EE. An ISE Shared Space, established by this component, would be a portion of the network infrastructure operated and maintained by this component and would provide an ISE-SAR EE interface on behalf of the entire organization. An example of such an implementation scheme is DHS's Regional Sharing System (RSS) that is under the responsibility of the Immigration and Customs Enforcement (ICE) agency providing bi-directional information sharing capabilities between the Federal Government and State and local partners.
- *Third Party Level:* ISE-SAR EE participants may leverage the services and infrastructure of another third party service provider, who is a member of the ISE-SAR EE community, for "virtually" establishing their ISE Shared Space. Such an implementation option should be consistent with overall concepts for an ISE Shared Space as outlined in the *ISE EAF* and this Segment Architecture. ISE-SAR EE participants, leveraging a third party service provider to host their ISE Shared Space, should have well-defined service level agreements (SLAs) to address the issues of resourcing, management, continuity of

operations, data stewardship, and ownership. If an ISE-SAR EE participant expects/intends to leverage a third party service provider, any and all implications for operations would not be the sole responsibility of the ISE-SAR EE third party service provider. For example, if Department X decides to permit another department or agency to host its data for sharing in the other department or agencies' ISE Shared Space, Department X remains ultimately responsible for the data stored and consumed within the third party resources servicing Department X's "virtual" ISE Shared Space.

3.2 Demonstrated ISE Core

Elements of the demonstrated ISE Core are resourced, planned, installed, and operated by designated ISE Implementation Agents supporting the ISE-SAR EE.[40] The ISE Implementation Agent's proposed enterprise, segment, and solutions architectures will clearly identify the structure and attributes that implement the demonstrated ISE Core segment in sufficient detail to support the investment and allow other ISE-SAR EE participants to plan their ISE Shared Spaces appropriately.

A number of key assumptions are made with regard to ISE Implementation Agents:

- Configuration management and systems integration are best accommodated with a single, designated ISE Implementation Agent (may also be called Service Provider) within each information security domain (i.e., TS/SCI, Secret/Collateral, and CUI/SBU). Robust configuration management processes must be in place in the event of multiple ISE Implementation Agents.
- Security policies and practices, whether originating in one community or not, must be ubiquitous within each security domain of the demonstrated ISE Core and between ISE Implementation Agents.
- Service Level Agreements (SLAs) will provide the necessary Quality of Service requirements and parameters for servicing the demonstrated ISE Core.

3.2.1 Hosting and Implementation Model

Various hosting and implementation options are available to establish the demonstrated ISE Core. These options include:

- *ISE Implementation Agent:* A designated primary ISE Implementation Agent is responsible for resourcing and providing all or a portion of the demonstrated ISE Core to ISE-SAR EE participants represented in the defense, homeland security, law enforcement, intelligence, and foreign affairs communities. Outsourcing of some services is an acceptable option, albeit SLAs should exist for all services, regardless of secondary outsourcing agents, to ensure Quality of Service is maintained across the ISE-SAR EE. Program management and operations oversight are the responsibility of the primary ISE Implementation Agent.
- *Single Community Implementation Agent:* A designated primary ISE Implementation Agent responsible for resourcing and providing all or a portion of the demonstrated ISE Core to ISE-SAR EE participants in a particular community (i.e., defense, homeland security, law

[40] For additional information, see *ISE EAF, Version 2.0* for a detailed discussion of ISE Implementation Agents and the ISE Core.

enforcement, intelligence, or foreign affairs). Outsourcing of some services is an acceptable option; albeit SLAs should exist for all services, regardless of secondary outsourcing agents, to ensure Quality of Service is maintained across the ISE-SAR EE. A joint SLA also should exist between the other communities and each single community ISE Implementation Agent. Program management and operations oversight over all ISE Implementation Agents is conducted through a designated department, agency, or other governmental organization.

- *Community Partnering Implementation Agent:* Two or more communities of ISE-SAR EE participants join together to identify and resource a designated primary service provider for their respective communities or share service provider responsibilities redundantly for enhanced performance (e.g., using Redundant Arrays of Inexpensive Disks [RAID]). Outsourcing of some demonstrated ISE Core services are an option; albeit SLAs should exist exclusively between this designated ISE Implementation Agent and other community ISE participants. A joint SLA should exist between ISE Implementation Agents with program management and operations oversight by a designated department, agency, or other governmental organization.

This page intentionally blank.